FileLocal

700 5th Avenue, Suite 4350
PO Box 94669
Seattle, WA 98124-4669

Executive Board:

Toni Call
City of Bellevue

Beth Anne Wroe
City of Des Moines

Susy Haugen
City of Everett

Lindsey Vaughn
City of Lake Forest Park

Jan Hawn
City of Renton

Glen Lee, Chair
City of Seattle

Andy Cherullo, Vice Chair
City of Tacoma

Executive Board Meeting Agenda

September 30, 2020

CONFERENCE CALL
SEATTLE, WA

1. **CALL TO ORDER**
   a. Introductions

2. **PUBLIC COMMENT***

3. **APPROVAL OF 05-28-20 MEETING SUMMARY**
   a. 05-28-20 Meeting Summary

4. **REVIEW OF AUGUST 2020, JULY 2020, JUNE 2020, AND MAY 2020 FINANCIAL STATEMENTS**
   a. August 2020 Financial Statements
   b. July 2020 Financial Statements
   c. June 2020 Financial Statements
   d. May 2020 Financial Statements

5. **ACTION ITEMS**
   a. Resolution **FL2020-07: Amendments to the Operations Manual** (Majority Vote)
      i. Briefing Paper: **FL2020-07**
      ii. Resolution: **FL2020-07**
      iii. Attachment A: **Operations Manual**
      iv. Attachment B: **Operations Manual (Redline)**
   b. Resolution FL2020-08 – **Leviathan Contract** (Majority Vote)
      v. Briefing Paper: **FL2020-08**
      vi. Resolution: **FL2020-08**
      vii. Attachment A: **Contract**

6. **OPERATIONAL UPDATES**
   a. MBR
   b. January 2020 Issues Update
   c. Agency/Vendor Performance Survey Update
   d. ADA Update
   e. New Cities Update
   f. Vendor warrants

*A public comment period is provided to allow the public to briefly present information, topics or issues that they feel should be considered by the board. Presentation should be limited to three minutes and be summary in nature. The board may decide to discuss the topic briefly at that time or to request its placement on a future agenda.

7. ADJOURNMENT

FileLocal

700 5th Avenue, Suite 4350
PO Box 94669
Seattle, WA 98124-4669

Executive Board Meeting Summary

May 28, 2020

CONFERENCE CALL

Executive Board:

Susy Haugen,
City of Everett

Toni Call, Chair
City of Bellevue

Beth Anne Wroe
City of Des Moines

Lindsey Vaughn
City of Lake Forest Park

Jan Hawn
City of Renton

Glen Lee, Chair
City of Seattle

Andy Cherullo, Vice-Chair
City of Tacoma

KEY: Underlined text indicates actions/decisions.
Bold/italicized text indicates follow up items.

Standing Items

1. CALL TO ORDER

The 05-28-20 meeting of the Washington Multi-City Business License and Tax Portal Agency (FileLocal) was called to order at 11:06 a.m. and conducted by conference call.

ROLL CALL

Board Members Present: Toni Call (phone), Beth Ann Wroe (phone) Sharon Fuller (phone) for Susy Haugen, Lindsey Vaughn (phone), Kari Roller, (phone) for Jan Hawn, and Glen Lee (phone)

Staff and Guests: David Linehan (phone), Kevin Fitzpatrick (phone), Wendy Thomaston (phone) and Julie Panick (phone)

2. PUBLIC COMMENT

There were no public comments.

3. APPROVAL OF MEETING SUMMARY

On a motion made by Toni Call and seconded by Glen Lee, the board approved the 04-17-20, meeting summary.

4. REVIEW OF FINANCIAL STATEMENT

Kevin Fitzpatrick summarized the April 2020 and March 2020 financial statements and cash status. There were no questions or comments.

5. ACTION ITEMS

A. Resolution FL2020-06: Draft Budget 2021-2025

a. Kevin Fitzpatrick reviewed the resolution. There were no questions or comments.

i. Motion to accept: Toni Call
ii. Motion seconded: Sharon Fuller
iii. Supermajority vote: Passed

*A public comment period is provided to allow the public to briefly present information, topics or issues that they feel should be considered by the board. Presentation should be limited to three minutes and be summary in nature. The board may decide to discuss the topic briefly at that time or to request its placement on a future agenda.

VOTE FL2020-06	City	Member
YES	Bellevue	Toni Call
YES	Des Moines	Beth Ann Wroe
YES	Everett	Sharon Fuller (for Susy Haugen)
YES	Lake Forest Park	Lindsey Vaughn
YES	Renton	Kari Roller (for Jan Hawn)
YES	Seattle	Glen Lee
Absent	Tacoma	Andy Cherullo

6. DISCUSSION ITEMS:

A. January 2020 Postmortem

Kevin Fitzpatrick reviewed the primary issues experienced during the January 2020 filing period and updated the status of work being done He stated that Avenu has formed a project team to address these issues and in addition he now meets with Avenu bi-weekly.

Kevin stated there are lots of changes in the Q'3 release. In response to a question from Kari Roller, Kevin stated that we are going to fully test before implementing these changes.

B. April Monthly Business Review

Kevin Fitzpatrick reviewed the Monthly Business Review. There were no comments or questions.

G. New Cities Update

Des Moines and Snoqualmie are on-track for Q'2 implementation. Kent will join FileLocal in 2021. Kevin has a follow-up call with Kent planned in June. There were no questions or comments.

H. Vendor Warrants

Program Manager expenses include $400 for the FileLocal Domain and the mileage expenses for quarterly city and new city meetings. There were no questions or comments.

7. ADJOURNMENT

On a motion made by Toni Call and seconded by Glen Lee the meeting the Executive Board adjourned at 11:47 a.m.

Respectfully Submitted,

Julie Panick
Secretary, FileLocal

700 5th Avenue, Suite 4350
PO Box 94669
Seattle, WA 98124-4669

FileLocal
Financial Statements
August 31, 2020

TABLE OF CONTENT	PAGE
STATEMENT OF FINANCIAL POSITION	1
STATEMENT OF ACTIVITIES	2
SCHEDULE OF BUDGET AND ACTUAL	3
STATEMENT OF CASH FLOW	4

Your one stop for local business licensing and tax filing

www.filelocal.org

FILELOCAL
STATEMENT OF FINANCIAL POSITION
AUGUST 31, 2020

ASSETS		
Cash	$	331,594
LGIP Investment		713,752
Accounts receivable		-
Dues from cities		14,849
Prepaid		60,042
Total Current Assets		1,120,237
TOTAL ASSETS	**$**	**1,120,237**
LIABILITIES AND NET ASSETS		
LIABILITIES		
Accounts payable	$	35,573
Accrued liabilities		104,355
Total Current Liabilities		139,928
TOTAL LIABILITIES		139,928
NET ASSETS		
Net assets, unrestricted		499,242
Change in net assets		481,067
TOTAL NET ASSETS		980,309
TOTAL LIABILITIES AND NET ASSETS	**$**	**1,120,237**

These financial statements have not been subjected to an audit or review or compilation engagement, and no assurance is provided on them.

Substantially all disclosures required by accounting principles generally accepted in the United States are not included.

FILELOCAL
STATEMENT OF ACTIVITIES
FOR THE MONTH
AND YEAR-TO-DATE ENDED AUGUST 31, 2020

	June	July	August	YTD
REVENUES				
User fees	$ 7,892	$ 54,724	$ 16,952	**$ 263,572**
Reimbursable cost/Capital cost recovery charges				
City of Seattle	-	-	-	**493,538**
City of Bellevue	-	-	-	**75,951**
City of Tacoma	-	-	-	**122,141**
City of Everett	-	-	-	**34,426**
City of Lake Forest Park	-	-	-	**9,093**
City of Bremerton	-	-	-	**38,825**
City of Renton	-	-	-	**39,773**
City of Shoreline	-	-	-	**15,597**
Total direct reimbursable costs	-	-	-	**829,344**
Total revenues	$ 7,892	$ 54,724	$ 16,952	**$ 1,092,916**
EXPENSES				
Accounting fees	$ 2,500	$ 2,500	$ 25,355	**$ 43,218**
Agency IT costs	-	-	-	**-**
Bank fees	33	7	-	**78**
Capital Recovery Payment	-	-	-	**-**
Conference cost	-	-	-	**-**
Consulting	-	-	-	**-**
Insurance	430	430	430	**3,417**
Labor costs	35,399	31,732	35,399	**251,945**
Legal fees	900	-	2,063	**11,033**
License and membership fees	-	-	-	**410**
Meals and entertainment	-	-	-	**-**
Office and operation supplies	-	-	-	**88**
Printing and copying	-	-	-	**-**
Technology costs	29,020	57,830	28,101	**170,396**
Transaction fees	(4,687)	24,495	2,792	**125,960**
Travel Expense	-	-	-	**213**
Other Expense	-	-	10	**5,091**
Total expenses	$ 63,595	$ 116,994	$ 94,150	**$ 611,849**
CHANGE IN NET ASSETS	$ (55,703)	$ (62,270)	$ (77,198)	**$ 481,067**

These financial statements have not been subjected to an audit or review or compilation engagement, and no assurance is provided on them.

Substantially all disclosures required by accounting principles generally accepted in the United States are not included.

FILELOCAL
SCHEDULE OF BUDGET AND ACTUAL
FOR THE YEAR TO DATE ENDED AUGUST 31, 2020

	Budget (Final)	YTD Budget	YTD Actual	Variance
REVENUES				
User fees	$ 395,010	$ 263,340	$ 263,572	$ 232
Reimbursable cost/Capital cost recovery charges				
City of Seattle	493,538	493,538	493,538	-
City of Bellevue	75,951	75,951	75,951	-
City of Tacoma	122,141	122,141	122,141	-
City of Everett	34,426	34,426	34,426	-
City of Lake Forest Park	9,093	9,093	9,093	-
City of Bremerton	38,825	38,825	38,825	-
City of Renton	39,773	39,773	39,773	-
City of Shoreline	15,597	15,597	15,597	-
Total direct reimbursable costs	829,344	829,344	829,344	-
Other				
Fund carryover	36,292	36,292	-	(36,292)
Total sources	$ 1,260,646	$ 1,128,976	$ 1,092,916	$ (36,060)
EXPENSES				
Labor costs	$ 424,786	$ 283,191	$ 251,945	$ 31,246
Contracts	61,044	40,697	46,713	(6,016)
Overhead	55,539	37,027	11,744	25,283
Technology costs	687,875	458,583	301,447	157,136
Operating reserve	11,402	7,601	-	7,601
Capital cost recovery payments	20,000	13,333	-	13,333
Total operating expenses	$ 1,260,646	$ 840,432	$ 611,849	$ 228,583
CHANGE IN NET ASSETS			481,067	
NET ASSETS, AS OF JANUARY 1, 2020			499,242	
NET ASSETS, AS OF AUGUST 31, 2020			$ 980,309	
Schedule I - Contracts				
Accounting	$ 41,740	$ 27,827	$ 43,218	$ (15,391)
Auditing	11,437	7,625	-	7,625
Insurance	6,291	4,194	3,417	777
Bank fees	1,576	1,051	78	973
Total Contracts	$ 61,044	$ 40,697	$ 46,713	$ (6,016)
Schedule II - Overhead				
Legal	$ 39,607	$ 26,405	$ 11,033	$ 15,372
Office and operating supplies	2,659	1,773	88	1,685
Printing	2,352	1,568	-	1,568
Licenses/Memberships	2,352	1,568	410	1,158
Agency IT costs	2,352	1,568	-	1,568
Marketing	6,217	4,145	213	3,932
Total Overhead	$ 55,539	$ 37,027	$ 11,744	$ 25,283

These financial statements have not been subjected to an audit or review or compilation engagement, and no assurance is provided on them.

Substantially all disclosures required by accounting principles generally accepted in the United States are not included.

FILELOCAL
STATEMENT OF CASHFLOW
FOR THE YEAR TO DATE ENDED AUGUST 31, 2020

		AUGUST 31, 2020
Change in Net Assets		$ 481,067
Adjustments to reconcile Change in Net Assets		
to net cash provided by operations:		
	Accounts Receivable	8,604
	Dues from Cities	83,441
	Prepaid	(59,747)
	Accounts Payable and Accrued Liabilities	(47,353)
Cash provided by operating activities		466,012
	Contributions to LGIP	(713,752)
Cash (used) for investing activities		(713,752)
Net cash increase (decrease)		(247,740)
Cash at January 1, 2020		579,334
Cash at August 31, 2020		**331,594**
Less Operating Reserve		**7,601**
Cash Available		**$ 323,993**

These financial statements have not been subjected to an audit or review or compilation engagement, and no assurance is provided on them.

Sustancially all disclosures required by accounting principles generally accepted in the United States are not included.

700 5th Avenue, Suite 4350
PO Box 94669
Seattle, WA 98124-4669

FileLocal
Financial Statements
July 31, 2020

TABLE OF CONTENT	PAGE
STATEMENT OF FINANCIAL POSITION	1
STATEMENT OF ACTIVITIES	2
SCHEDULE OF BUDGET AND ACTUAL	3
STATEMENT OF CASH FLOW	4

Your one stop for local business licensing and tax filing

www.filelocal.org

FILELOCAL
STATEMENT OF FINANCIAL POSITION
JULY 31, 2020

ASSETS		
Cash	$	458,579
LGIP Investment		713,752
Accounts receivable		-
Dues from cities		14,849
Prepaid		74,972
Total Current Assets		1,262,152
TOTAL ASSETS	**$**	**1,262,152**
LIABILITIES AND NET ASSETS		
LIABILITIES		
Accounts payable	$	128,481
Accrued liabilities		76,164
Total Current Liabilities		204,645
TOTAL LIABILITIES		204,645
NET ASSETS		
Net assets, unrestricted		499,242
Change in net assets		558,265
TOTAL NET ASSETS		1,057,507
TOTAL LIABILITIES AND NET ASSETS	**$**	**1,262,152**

These financial statements have not been subjected to an audit or review or compilation engagement, and no assurance is provided on them.

Substantially all disclosures required by accounting principles generally accepted in the United States are not included.

FILELOCAL
STATEMENT OF ACTIVITIES
FOR THE MONTH
AND YEAR-TO-DATE ENDED JULY 31, 2020

	May	June	July	YTD
REVENUES				
User fees	$ 20,392	$ 7,892	$ 54,724	**$ 246,620**
Reimbursable cost/Capital cost recovery charges				
City of Seattle	-	-	-	**493,538**
City of Bellevue	-	-	-	**75,951**
City of Tacoma	-	-	-	**122,141**
City of Everett	-	-	-	**34,426**
City of Lake Forest Park	-	-	-	**9,093**
City of Bremerton	-	-	-	**38,825**
City of Renton	-	-	-	**39,773**
City of Shoreline	-	-	-	**15,597**
Total direct reimbursable costs	-	-	-	**829,344**
Total revenues	$ 20,392	$ 7,892	$ 54,724	**$ 1,075,964**
EXPENSES				
Accounting fees	$ 2,500	$ 2,500	$ 2,500	**$ 17,863**
Agency IT costs	-	-	-	**-**
Bank fees	17	33	7	**78**
Capital Recovery Payment	-	-	-	**-**
Conference cost	-	-	-	**-**
Consulting	-	-	-	**-**
Insurance	430	430	430	**2,987**
Labor costs	35,399	35,399	31,732	**216,546**
Legal fees	1,680	900	-	**8,970**
License and membership fees	-	-	-	**410**
Meals and entertainment	-	-	-	**-**
Office and operation supplies	-	-	-	**88**
Printing and copying	-	-	-	**-**
Technology costs	18,075	29,020	57,830	**142,295**
Transaction fees	15,977	(4,687)	24,495	**123,168**
Travel Expense	-	-	-	**213**
Other Expense	-	-	-	**5,081**
Total expenses	$ 74,078	$ 63,595	$ 116,994	**$ 517,699**
CHANGE IN NET ASSETS	$ (53,686)	$ (55,703)	$ (62,270)	**$ 558,265**

These financial statements have not been subjected to an audit or review or compilation engagement, and no assurance is provided on them.

Substantially all disclosures required by accounting principles generally accepted in the United States are not included.

FILELOCAL
SCHEDULE OF BUDGET AND ACTUAL
FOR THE YEAR TO DATE ENDED JULY 31, 2020

	Budget (Final)	YTD Budget	YTD Actual	Variance
REVENUES				
User fees	$ 395,010	$ 230,423	$ 246,620	$ 16,197
Reimbursable cost/Capital cost recovery charges				
City of Seattle	493,538	493,538	493,538	-
City of Bellevue	75,951	75,951	75,951	-
City of Tacoma	122,141	122,141	122,141	-
City of Everett	34,426	34,426	34,426	-
City of Lake Forest Park	9,093	9,093	9,093	-
City of Bremerton	38,825	38,825	38,825	-
City of Renton	39,773	39,773	39,773	-
City of Shoreline	15,597	15,597	15,597	-
Total direct reimbursable costs	829,344	829,344	829,344	-
Other				
Fund carryover	36,292	36,292	-	(36,292)
Total sources	$ 1,260,646	$ 1,096,059	$ 1,075,964	$ (20,095)
EXPENSES				
Labor costs	$ 424,786	$ 247,792	$ 216,546	$ 31,246
Contracts	61,044	35,609	20,928	14,681
Overhead	55,539	32,398	9,681	22,717
Technology costs	687,875	401,260	270,544	130,716
Operating reserve	11,402	6,651	-	6,651
Capital cost recovery payments	20,000	11,667	-	11,667
Total operating expenses	$ 1,260,646	$ 735,377	$ 517,699	$ 217,678
CHANGE IN NET ASSETS			558,265	
NET ASSETS, AS OF JANUARY 1, 2020			499,242	
NET ASSETS, AS OF JULY 31, 2020			$ 1,057,507	
Schedule I - Contracts				
Accounting	$ 41,740	$ 24,348	$ 17,863	$ 6,485
Auditing	11,437	6,672	-	6,672
Insurance	6,291	3,670	2,987	683
Bank fees	1,576	919	78	841
Total Contracts	$ 61,044	$ 35,609	$ 20,928	$ 14,681
Schedule II - Overhead				
Legal	$ 39,607	$ 23,104	$ 8,970	$ 14,134
Office and operating supplies	2,659	1,551	88	1,463
Printing	2,352	1,372	-	1,372
Licenses/Memberships	2,352	1,372	410	962
Agency IT costs	2,352	1,372	-	1,372
Marketing	6,217	3,627	213	3,414
Total Overhead	$ 55,539	$ 32,398	$ 9,681	$ 22,717

These financial statements have not been subjected to an audit or review or compilation engagement, and no assurance is provided on them.

Substantially all disclosures required by accounting principles generally accepted in the United States are not included.

FILELOCAL
STATEMENT OF CASHFLOW
FOR THE YEAR TO DATE ENDED JULY 31, 2020

		JULY 31, 2020
Change in Net Assets		$ 558,265
Adjustments to reconcile Change in Net Assets		
to net cash provided by operations:		
	Accounts Receivable	8,604
	Dues from Cities	83,441
	Prepaid	(74,677)
	Accounts Payable and Accrued Liabilities	17,364
Cash provided by operating activities		592,997
	Contributions to LGIP	(713,752)
Cash (used) for investing activities		(713,752)
Net cash increase (decrease)		(120,755)
Cash at January 1, 2020		579,334
Cash at July 31, 2020		**458,579**
Less Operating Reserve		**6,651**
Cash Available		**$ 451,928**

These financial statements have not been subjected to an audit or review or compilation engagement, and no assurance is provided on them.

Sustancially all disclosures required by accounting principles generally accepted in the United States are not included.

700 5th Avenue, Suite 4350
PO Box 94669
Seattle, WA 98124-4669

FileLocal
Financial Statements
June 30, 2020

TABLE OF CONTENT	PAGE
STATEMENT OF FINANCIAL POSITION	1
STATEMENT OF ACTIVITIES	2
SCHEDULE OF BUDGET AND ACTUAL	3
STATEMENT OF CASH FLOW	4

Your one stop for local business licensing and tax filing

www.filelocal.org

FILELOCAL
STATEMENT OF FINANCIAL POSITION
JUNE 30, 2020

ASSETS		
Cash	$	963,752
Accounts receivable		198,092
Dues from cities		14,849
Prepaid		89,902
Total Current Assets		1,266,595
TOTAL ASSETS	**$**	**1,266,595**
LIABILITIES AND NET ASSETS		
LIABILITIES		
Accounts payable	$	22,662
Accrued liabilities		124,157
Total Current Liabilities		146,819
TOTAL LIABILITIES		146,819
NET ASSETS		
Net assets, unrestricted		499,242
Change in net assets		620,534
TOTAL NET ASSETS		1,119,776
TOTAL LIABILITIES AND NET ASSETS	**$**	**1,266,595**

These financial statements have not been subjected to an audit or review or compilation engagement, and no assurance is provided on them.

Substantially all disclosures required by accounting principles generally accepted in the United States are not included.

FILELOCAL
STATEMENT OF ACTIVITIES
FOR THE MONTH
AND YEAR-TO-DATE ENDED JUNE 30, 2020

	April	May	June	YTD
REVENUES				
User fees	$ 45,260	$ 20,392	$ 7,892	**$ 191,896**
Reimbursable cost/Capital cost recovery charges				
City of Seattle	493,538	-	-	**493,538**
City of Bellevue	75,951	-	-	**75,951**
City of Tacoma	122,141	-	-	**122,141**
City of Everett	34,426	-	-	**34,426**
City of Lake Forest Park	9,093	-	-	**9,093**
City of Bremerton	38,825	-	-	**38,825**
City of Renton	39,773	-	-	**39,773**
City of Shoreline	15,597	-	-	**15,597**
Total direct reimbursable costs	829,344	-	-	**829,344**
Total revenues	$ 874,604	$ 20,392	$ 7,892	**$ 1,021,240**
EXPENSES				
Accounting fees	$ 2,500	$ 2,500	$ 2,500	**$ 15,363**
Agency IT costs	-	-	-	**-**
Bank fees	2	17	33	**71**
Capital Recovery Payment	-	-	-	**-**
Conference cost	-	-	-	**-**
Consulting	-	-	-	**-**
Insurance	430	430	430	**2,557**
Labor costs	26,532	35,399	35,399	**184,814**
Legal fees	960	1,680	900	**8,970**
License and membership fees	300	-	-	**410**
Meals and entertainment	-	-	-	**-**
Office and operation supplies	5	-	-	**88**
Printing and copying	-	-	-	**-**
Technology costs	(6,529)	18,075	29,020	**84,465**
Transaction fees	39,776	15,977	(4,687)	**98,674**
Travel Expense	27	-	-	**213**
Other Expense	-	-	-	**5,081**
Total expenses	$ 64,003	$ 74,078	$ 63,595	**$ 400,706**
CHANGE IN NET ASSETS	$ 810,601	$ (53,686)	$ (55,703)	**$ 620,534**

These financial statements have not been subjected to an audit or review or compilation engagement, and no assurance is provided on them.

Substantially all disclosures required by accounting principles generally accepted in the United States are not included.

FILELOCAL
SCHEDULE OF BUDGET AND ACTUAL
FOR THE YEAR TO DATE ENDED JUNE 30, 2020

	Budget (Final)	YTD Budget	YTD Actual	Variance
REVENUES				
User fees	$ 395,010	$ 197,505	$ 191,896	$ (5,609)
Reimbursable cost/Capital cost recovery charges				
City of Seattle	493,538	493,538	493,538	-
City of Bellevue	75,951	75,951	75,951	-
City of Tacoma	122,141	122,141	122,141	-
City of Everett	34,426	34,426	34,426	-
City of Lake Forest Park	9,093	9,093	9,093	-
City of Bremerton	38,825	38,825	38,825	-
City of Renton	39,773	39,773	39,773	-
City of Shoreline	15,597	15,597	15,597	-
Total direct reimbursable costs	829,344	829,344	829,344	-
Other				
Fund carryover	36,292	36,292	-	(36,292)
Total sources	$ 1,260,646	$ 1,063,141	$ 1,021,240	$ (41,901)
EXPENSES				
Labor costs	$ 424,786	$ 212,393	$ 184,814	$ 27,579
Contracts	61,044	30,522	17,991	12,531
Overhead	55,539	27,770	9,681	18,089
Technology costs	687,875	343,938	188,220	155,718
Operating reserve	11,402	5,701	-	5,701
Capital cost recovery payments	20,000	10,000	-	10,000
Total operating expenses	$ 1,260,646	$ 630,324	$ 400,706	$ 229,618
CHANGE IN NET ASSETS			620,534	
NET ASSETS, AS OF JANUARY 1, 2020			499,242	
NET ASSETS, AS OF JUNE 30, 2020			$ 1,119,776	
Schedule I - Contracts				
Accounting	$ 41,740	$ 20,870	$ 15,363	$ 5,507
Auditing	11,437	5,719	-	5,719
Insurance	6,291	3,146	2,557	589
Bank fees	1,576	788	71	717
Total Contracts	$ 61,044	$ 30,523	$ 17,991	$ 12,532
Schedule II - Overhead				
Legal	$ 39,607	$ 19,804	$ 8,970	$ 10,834
Office and operating supplies	2,659	1,330	88	1,242
Printing	2,352	1,176	-	1,176
Licenses/Memberships	2,352	1,176	410	766
Agency IT costs	2,352	1,176	-	1,176
Marketing	6,217	3,109	213	2,896
Total Overhead	$ 55,539	$ 27,771	$ 9,681	$ 18,090

These financial statements have not been subjected to an audit or review or compilation engagement, and no assurance is provided on them.

Substantially all disclosures required by accounting principles generally accepted in the United States are not included.

FILELOCAL
STATEMENT OF CASHFLOW
FOR THE YEAR TO DATE ENDED JUNE 30, 2020

		JUNE 30, 2020
Change in Net Assets		$ 620,534
Adjustments to reconcile Change in Net Assets		
to net cash provided by operations:		
	Accounts Receivable	(189,488)
	Dues from Cities	83,441
	Prepaid	(89,607)
	Accounts Payable and Accrued Liabilities	(40,463)
Net cash increase for one months ending June 30, 2020		384,418
Cash at January 1, 2020		579,334
Cash at June 30, 2020		**963,752**
Less Operating Reserve		**5,701**
Cash Available		**$ 958,051**

These financial statements have not been subjected to an audit or review or compilation engagement, and no assurance is provided on them.

Sustancially all disclosures required by accounting principles generally accepted in the United States are not included.

700 5th Avenue, Suite 4350
PO Box 94669
Seattle, WA 98124-4669

FileLocal
Financial Statements
May 31, 2020

TABLE OF CONTENT	PAGE
STATEMENT OF FINANCIAL POSITION	1
STATEMENT OF ACTIVITIES	2
SCHEDULE OF BUDGET AND ACTUAL	3
STATEMENT OF CASH FLOW	4

Your one stop for local business licensing and tax filing

www.filelocal.org

FILELOCAL
STATEMENT OF FINANCIAL POSITION
MAY 31, 2020

ASSETS		
Cash	$	405,481
Accounts receivable		691,630
Dues from cities		87,772
Prepaid		104,833
Total Current Assets		1,289,716
TOTAL ASSETS	**$**	**1,289,716**
LIABILITIES AND NET ASSETS		
LIABILITIES		
Accounts payable	$	23,292
Accrued liabilities		90,945
Total Current Liabilities		114,237
TOTAL LIABILITIES		114,237
NET ASSETS		
Net assets, unrestricted		499,242
Change in net assets		676,237
TOTAL NET ASSETS		1,175,479
TOTAL LIABILITIES AND NET ASSETS	**$**	**1,289,716**

These financial statements have not been subjected to an audit or review or compilation engagement, and no assurance is provided on them.

Substantially all disclosures required by accounting principles generally accepted in the United States are not included.

FILELOCAL
STATEMENT OF ACTIVITIES
FOR THE MONTH
AND YEAR-TO-DATE ENDED MAY 31, 2020

	March	April	May	YTD
REVENUES				
User fees	$ 9,844	$ 45,260	$ 20,392	**$ 184,004**
Reimbursable cost/Capital cost recovery charges				
City of Seattle	-	493,538	-	**493,538**
City of Bellevue	-	75,951	-	**75,951**
City of Tacoma	-	122,141	-	**122,141**
City of Everett	-	34,426	-	**34,426**
City of Lake Forest Park	-	9,093	-	**9,093**
City of Bremerton	-	38,825	-	**38,825**
City of Renton	-	39,773	-	**39,773**
City of Shoreline	-	15,597	-	**15,597**
Total direct reimbursable costs	-	829,344	-	**829,344**
Total revenues	$ 9,844	$ 874,604	$ 20,392	**$ 1,013,348**
EXPENSES				
Accounting fees	$ 2,863	$ 2,500	$ 2,500	**$ 12,863**
Agency IT costs	-	-	-	**-**
Bank fees	10	2	17	**38**
Capital Recovery Payment	-	-	-	**-**
Conference cost	-	-	-	**-**
Consulting	-	-	-	**-**
Insurance	430	430	430	**2,127**
Labor costs	35,399	26,532	35,399	**149,415**
Legal fees	4,980	960	1,680	**8,070**
License and membership fees	-	300	-	**410**
Meals and entertainment	-	-	-	**-**
Office and operation supplies	83	5	-	**88**
Printing and copying	-	-	-	**-**
Technology costs	14,500	(6,529)	18,075	**55,446**
Transaction fees	3,692	39,776	15,977	**103,360**
Travel Expense	-	27	-	**213**
Other Expense	-	-	-	**5,081**
Total expenses	$ 61,957	$ 64,003	$ 74,078	**$ 337,111**
CHANGE IN NET ASSETS	$ (52,113)	$ 810,601	$ (53,686)	**$ 676,237**

These financial statements have not been subjected to an audit or review or compilation engagement, and no assurance is provided on them.

Substantially all disclosures required by accounting principles generally accepted in the United States are not included.

FILELOCAL
SCHEDULE OF BUDGET AND ACTUAL
FOR THE YEAR TO DATE ENDED MAY 31, 2020

	Budget (Final)	YTD Budget	YTD Actual	Variance
REVENUES				
User fees	$ 395,010	$ 164,588	$ 184,004	$ 19,416
Reimbursable cost/Capital cost recovery charges				
City of Seattle	493,538	493,538	493,538	-
City of Bellevue	75,951	75,951	75,951	-
City of Tacoma	122,141	122,141	122,141	-
City of Everett	34,426	34,426	34,426	-
City of Lake Forest Park	9,093	9,093	9,093	-
City of Bremerton	38,825	38,825	38,825	-
City of Renton	39,773	39,773	39,773	-
City of Shoreline	15,597	15,597	15,597	-
Total direct reimbursable costs	829,344	829,344	829,344	-
Other				
Fund carryover	36,292	36,292	-	(36,292)
Total sources	$ 1,260,646	$ 1,030,224	$ 1,013,348	$ (16,876)
EXPENSES				
Labor costs	$ 424,786	$ 176,994	$ 149,415	$ 27,579
Contracts	61,044	25,435	15,028	10,407
Overhead	55,539	23,141	8,781	14,360
Technology costs	687,875	286,615	163,887	122,728
Operating reserve	11,402	4,751	-	4,751
Capital cost recovery payments	20,000	8,333	-	8,333
Total operating expenses	$ 1,260,646	$ 525,269	$ 337,111	$ 188,158
CHANGE IN NET ASSETS			676,237	
NET ASSETS, AS OF JANUARY 1, 2020			499,242	
NET ASSETS, AS OF MAY 31, 2020			$ 1,175,479	
Schedule I - Contracts				
Accounting	$ 41,740	$ 17,392	$ 12,863	$ 4,529
Auditing	11,437	4,765	-	4,765
Insurance	6,291	2,621	2,127	494
Bank fees	1,576	657	38	619
Total Contracts	$ 61,044	$ 25,435	$ 15,028	$ 10,407
Schedule II - Overhead				
Legal	$ 39,607	$ 16,503	$ 8,070	$ 8,433
Office and operating supplies	2,659	1,108	88	1,020
Printing	2,352	980	-	980
Licenses/Memberships	2,352	980	410	570
Agency IT costs	2,352	980	-	980
Marketing	6,217	2,590	213	2,377
Total Overhead	$ 55,539	$ 23,141	$ 8,781	$ 14,360

These financial statements have not been subjected to an audit or review or compilation engagement, and no assurance is provided on them.

Substantially all disclosures required by accounting principles generally accepted in the United States are not included.

FILELOCAL
STATEMENT OF CASHFLOW
FOR THE YEAR TO DATE ENDED MAY 31, 2020

		May 31, 2020
Change in Net Assets		$ 676,237
Adjustments to reconcile Change in Net Assets		
to net cash provided by operations:		
	Accounts Receivable	(683,026)
	Dues from Cities	10,517
	Prepaid	(104,537)
	Accounts Payable and Accrued Liabilities	(73,045)
Net cash increase for one months ending May 31, 2020		(173,853)
Cash at January 1, 2020		579,334
Cash at May 31, 2020		**405,481**
Less Operating Reserve		**11,402**
Cash Available		**$ 394,079**

These financial statements have not been subjected to an audit or review or compilation engagement, and no assurance is provided on them.

Sustancially all disclosures required by accounting principles generally accepted in the United States are not included.

FileLocal

700 5th Avenue, Suite 4350
PO Box 94669
Seattle, WA 98124-4669

File Local Resolution FL2020-07
Briefing Paper: Amendments to the Agency Operations Manual

Date: September 30, 2020

Issue: Shall the Washington Multi-City Business License and Tax Portal Agency ("Agency") Executive Board approve revisions to the Operations Manual as recommended by the Program Manager and Operations Committee?

Operating Committee Recommendation: The Portal Agency Executive Board should pass Resolution FL2020-07 to adopt an updated Operations Manual incorporating the following changes as recommended by the Program Manager and Operations Committee:

- Fiscal Manual – revision to allow excess funds to be placed with the Washington State Local Government Investment Pool (LGIP)
- IT Manual – minor revisions to IT policies as identified by the Agency's security vendor
- Electronic Signature Policy – to allow the use of electronic signatures with certain Agency documents, using Adobe Sign or an equivalent technology platform.
- Other minor substantive, technical, and formatting revisions to harmonize Agency policies and incorporate new information since the previous update.

Rationale: It is important for Agency operations policies and procedures to reflect current best practices and to ensure the efficient

functioning of the Agency and its process. The recommended revisions to the Operations Manual correspond with recently approved changes to use of excess funds and reflect the input of the Agency's IT security consultant. The revisions to the Electronic Signature Policy will enable more secure and efficient handling of Agency resolutions, contracts, and other important documents, particularly while Agency personnel and vendors are working remotely.

RESOLUTION NO. FL2020-07

A Resolution of the Washington Multi-City Business License and Tax Portal Agency Executive Board Approving Amendments to the Agency Operations Manual.

Whereas, the Agency's administrative and internal operations are governed by certain policies and procedures previously adopted by the Executive Board and compiled into a single document known as the Operations Manual, which has been revised from time to time upon the recommendations of the Program Manager and Operations Committee; and

Whereas, the Program Manager and the Operations Committee have again recommended a number of changes to the Agency's Operations Manual, including substantial revisions to the portions of the manual known as the Fiscal Manual, the IT Manual, and the Electronic Signature Policy, along with other minor substantive, technical, and formatting changes; and

Whereas, an updated version of the Operations Manual, including all of the recommended changes, is shown in Exhibit A hereto; and for ease of reference, the proposed changes are shown in redline comparison format in Exhibit B hereto; and

Whereas, the Executive Board concurs that the recommended changes to the Operations Manual are appropriate and will improve the operating efficiency and day-to-day functioning of the Agency;

Now, therefore,

BE IT RESOLVED by the Executive Board of the Washington Multi-City Business License and Tax Portal Agency as follows:

SECTION 1. The FileLocal Operations Manual is hereby amended to incorporate the changes recommended by the Program Manager and Operations Committee. The former version of the Operations Manual shall be replaced with the updated version shown in Exhibit A hereto. This updated Operations Manual includes substantial revisions to the Fiscal Manual, the IT Manual, and the Electronic Signature Policy, as well as minor revisions, technical corrections, and formatting changes to other sections of the prior Operations Manual.

SECTION 2. The updated FileLocal Operations Manual shall be in full force and effect immediately upon adoption of this Resolution.

ADOPTED this 30th day of September, 2020.

ATTEST:

Washington Multi-City Business License and Tax Portal Agency Executive Board
Seattle, Washington

Board Secretary

Board Chair

FileLocal

Your one stop for local business licensing and tax filing

www.filelocal.org

OPERATIONS POLICIES & PROCEDURES

September 2020

TABLE OF CONTENTS

Introduction

Purpose 3

Overview 3
Guiding Principles 3
Business Structure 4

Roles, Rules and Responsibilities

Executive Board Meetings 5
Executive Board Membership, Terms, Quorum, Voting 5
Overview of Roles and Responsibilities 6

Operational Procedures

Communications Protocols 8
Conflict of Interest Policy 12
Emergency Procedures 20
Fiscal Manual 21
Information Technology Securities Policy Manual 47
Public Records Policy 116
Use of Electronic Signatures 121

Appendices

A. Key Governance Documentation 124
A1. Articles of Incorporation 125
A2. Interlocal Agreement 136
A3. Bylaws 181
B. Organizational Chart, Roster 194
C. Delegation of Authorities 195
D. Executive Board Meeting Schedules 197

Introduction

Purpose

The FileLocal Operations Manual has several purposes: to help guide FileLocal leaders, staff and city partners in developing and sustaining a successful enterprise; to document procedures and policies; to support agency accountability and efficiency; and to serve as a reference for questions and problems as they arise in day-to-day operations.

Overview

FileLocal's primary purpose is to offer a web-based service that will make it easier for businesses to obtain a business license and pay local taxes to its member cities.

FileLocal is a municipal corporation authorized by state law to issue local business licenses and collect a variety of local taxes. It was formed to make it easier and more efficient for businesses to apply for local business licenses and file local taxes while allowing cities to retain local control over licensing and tax collection functions and policies. The Principal cities – Bellevue, Everett, Seattle, and Tacoma – jointly facilitated the creation of an internet web application gateway (a "portal") where tax collection and business licensing functions can be collectively administered, and where businesses operating in multiple cities can use a "one-stop" system for tax payment or business license application filing.

Guiding Principles

The principles guiding FileLocal reflect integrity, accountability, local control, flexibility, accessibility, security, and affordability for cities, businesses, and taxpayers:

- Integrity: FileLocal will be honest, truthful, and straightforward.
- Accountability: FileLocal will be responsible for its actions and decisions, a good steward of public funds and transparent in its operations.
- Local Control: FileLocal will seek to respect and preserve each participating city's authority to set local tax policies.
- Flexibility: FileLocal will strive to nimbly respond to a changing business, technology, and policy environment.
- Accessibility: FileLocal will seek to be accessible and responsive to taxpayers, licensees, and participating cities.
- Security: FileLocal will at all times seek to safeguard taxpayer, licensee, and participating city data.
- Affordability: FileLocal will seek to be affordable to both Participating Cities and businesses and taxpayers using the portal. Also, fees and charges will be structured so that the addition of new cities using the portal does not impose additional costs on prior participating cities.

Business Structure

FileLocal is a public agency formed as a nonprofit corporation as authorized by the state Interlocal Cooperation Act (39.34 RCW) and the Nonprofit Misc. & Mutual Corporations Act (24.06 RCW). FileLocal is an instrumentality of its member cities formed to carry out exclusively governmental activities. The four founding cities are Bellevue, Everett, Seattle, and Tacoma. The legal name of the agency is the "Washington Multi-City Business Licenses and Tax Portal Agency."

The four founding cities are the "Principals" and have representation on the Executive Board, which governs the agency. Additional Washington cities may apply to join FileLocal, either as a Principal or as a Subscriber. Principals have voting rights on the Executive Board; Subscribers have nonvoting representation on the Executive Board.

Roles, Rules, and Responsibilities

EXECUTIVE BOARD MEETINGS

All Meetings will be held at the Seattle Municipal Tower (SMT) and via Skype. These meetings are open to the public in compliance with the Washington State Open Public Meetings Act (42.30 RCW). Meeting dates, times, locations, materials, and summaries are posted on filelocal.org. Unless otherwise noted, meetings are held in SMT 4070 at 12:00 pm. Skype meeting information is for Board members only; the public must attend in person.

EXECUTIVE BOARD MEMBERSHIP, TERMS, QUORUM, VOTING

This document is meant to be a summary of the more detailed descriptions provided in the FileLocal ILA and Bylaws.

MEMBERSHIP

- The FileLocal Board consists of one representative from each Principal city
- Individuals must be a Chief Financial Officer or their deputy or equivalent
- Alternates are designated in writing and must meet same qualifications

TERMS

- Unless the member resigns or is removed in accordance with the Bylaws, each member holds office until replaced by resolution or written motion of the legislative body of the appointing Principal
- Board members representing multiple principals are selected biennially

QUORUM

- A simple majority of members (or their alternates)

VOTING

- Each member has one vote
- A "Supermajority Vote' means Executive Board approval of an item accomplished by securing affirmative votes of not less than sixty-six percent (66%) of all voting Board Members of the Executive Board in number, and not less than sixty-six percent (66%) in number of the Original Principals (the Cities of Bellevue, Everett, Seattle, and Tacoma) [i.e., 3 out of 4]. Generally, items requiring supermajority vote for approval involve the following:
  - Budget, user fees/charges
  - Operations policies
  - Major docs: Bylaws, Articles of Incorporation, ILA
  - Decisions with significant financial impact (e.g., contracts over $50,000)
  - Adding or removing people (New principals or subscribers, adding seats, adding staff positions, removing the manager)
  - Merging, sale, dissolving

Table 1:OVERVIEW OF ROLES AND RESPONSIBILITIES

PRINCIPAL CITIES	ROLE: Incorporators
Accountable to	Voters

EXECUTIVE BOARD	ROLE: Governing Body
Accountable to	State, pursuant to Interlocal Cooperation Act (39.34 RCW)
Responsibilities	• Final decision-making authority on policy issues • Recommending action to participating city legislative bodies • Review/approve budget and budget policies • Review/adopt personnel, operating, financial policies • Direct/supervise committees/advisory boards • Conduct regular and special meetings • Manage/maintain records • Determine services offered/ terms • Approve new principals and subscribers • Establish fund or special funds Retain/terminate manager • Create committees • Enter into agreements • Establish fees • Approve strategic plans • Accept funds • Receive property (et. al.) • Sue and be sued • Make/alter bylaws

OPERATIONS COMMITTEE	ROLE: Advise and Recommend
Accountable to	Executive Board
Responsibilities	• Assist in review/development of operations policy, development options, proposed new services, other matters as directed • Provide advice, information, and recommendations to staff • Assist in review/development of budget • Assist in communications • Reach out to tech staff within cities • Brief Executive Board members

PROGRAM MANAGER	ROLE: Manage Agency
Accountable to	Executive Board
Responsibilities	• Ensure overall compliance of agency with laws and regulations • Management of staff and technology vendors • Quality control and operations of portal • Administrative support of board • External relations

LEGAL	ROLE: Legal Counsel
Accountable to	Executive Board and Program Manager
Responsibilities	Review resolutions and contracts; ensure legal compliance

ACCOUNTING	ROLE: Financial Compliance
Accountable to	Executive Board and Program Manager
Responsibilities	Prepare and manage financial reports; support audits as required

TECHNOLOGY VENDORS	ROLE: Portal Technological Management
Accountable to	Program Manager
Responsibilities	Manage portal, handle payments, ensure information security

COMMUNICATIONS	ROLE: Manage City Communications
Accountable to	Executive Board
Responsibilities	Manage city's communications and coordinate with other cities on joint communications

INTERGOVERNMENTAL RELATIONS	ROLE: Lobbyists
Accountable to	Executive Board
Responsibilities	Lobby state government legislators on behalf of cities and agency

Communications Protocols

1. Purpose

Ensuring that taxpayers and the general public receive timely and accurate information regarding FileLocal is a communication priority. The FileLocal staff and cities are charged with communicating with external audiences about FileLocal. The FileLocal program manager coordinates communications and relies on partner cities' communication resources. Effective communication requires strategic direction, coordination and clear roles and responsibilities.

2. Policy

All parties commit to act in good faith in seeking to work together in an open and forthright manner. Communications between the parties will be early and frequent to guarantee strong coordination, maximize opportunities and minimize surprises. The public will not typically distinguish between FileLocal and the individual cities. It will benefit all parties to work cooperatively to inform the public that we are effectively and safely providing the level of services people expect and deserve.

FileLocal and the cities will coordinate communications to ensure:

A. Timely information is easily accessible to businesses and the public.

B. Communication goals are met.

C. Messages are consistent.

D. Appropriate credit is shared.

3. Background

- FileLocal offers a web-based service that will make it easier for businesses to obtain a business license and pay local taxes, for multiple cities, from one website
- FileLocal is a municipal corporation authorized by state law to issue local business licenses and collect a variety of local taxes.
- FileLocal makes it easier and more efficient for businesses to apply for local business licenses and file local taxes while allowing cities to retain local control over licensing and tax collection functions and policies.
- The Principal cities – Bellevue, Everett, Seattle, and Tacoma – jointly facilitated the creation of FileLocal.

4. Roles

- The FileLocal Program Manager is the communications lead, primary spokesperson, and media contact for FileLocal. The Program Manager is provided through a Service Level Agreement between the City of Seattle and FileLocal. If the Program Manager is not available, the role defers to the FileLocal Executive Board Chair (Reference Appendix B).

- An Executive Board (Board) governs FileLocal (a not-for-profit corporation under Washington law, formed as Washington Multi-City Business License and Tax Portal Agency). As such, it provides leadership and overall direction on FileLocal communications. The Board is comprised of seven directors, representing each of the principal cities (Reference Appendix B)
    - City of Bellevue
    - City of Des Moines
    - City of Everett
    - City of Lake Forest Park
    - City of Renton
    - City of Seattle
    - City of Tacoma
- FileLocal's technical providers (vendors) are Avenu, KUBRA, and Leviathan.

5. Protocols

A. The following protocols serve as guidelines for communicating effectively with external audiences. The protocols are intended to be fluid – capable of reacting to feedback and changes as needed. The protocols should be reviewed regularly to ensure that they are effective and appropriate as needs change. Activities include, but are not limited to:

I. Providing information to businesses/citizens/public
II. Providing information to other cities/units of government
III. Meeting requests and correspondence
IV. Media relations
V. Materials, including content development and production of digital, print, signage and identity
VI. Coordination with the public, agencies, consultants, vendors, etc.

B. External communications with the public, stakeholders and the media will be coordinated by the FileLocal Program Manager to leverage resources, ensure accuracy of information and to minimize surprises. City/Executive communication staff will be included in information sharing so that they are prepared to respond.

C. As the governing body, the FileLocal Board will review policy, finance, and planning-related communications.

D. As the service provider, the Program Manager will lead operations-related communications. This includes but is not limited to communications related to:

I. Project preparation, testing, launch, and maintenance
II. Ongoing services
III. Operations, contractors, and personnel

E. Service incident protocols are being developed by Avenu. Please refer to these separate protocols for additional detail.

F. Production of materials will be coordinated and reviewed by the Program Manager to ensure accuracy.

I. The FileLocal logo will be included on all communication materials. Principal city logos should only be added when the material reflects a jointly sponsored event.

II. Boilerplate language agreed upon by all parties describing the relationship between the cities and FileLocal will be included. (FileLocal is an easy and flexible online tool that provides a streamlined approach to applying for business licenses and filing local taxes with any Washington member city.)

III. Development of materials will be assigned appropriately to utilize expertise and leverage resources efficiently. The lead entity will be responsible for generating first drafts of materials.

IV. All drafts will be reviewed and approved by the Program Manager before distribution.

V. Every effort to provide reasonable review time will be provided (taking into account unforeseen circumstances or constraints). Similarly, timely approval of materials is expected.

G. Contacts will be alerted of all media contacts and meeting requests and be provided a brief summary of the interaction in a timely manner.

I. Reporter or organization name and contact information

II. Summary of the request and deadline

III. Coordination between FileLocal and cities on appropriate and available spokesperson

IV. Follow-up to confirm reporter or organization has received a response

H. FileLocal will maintain project information on its website. It will work with cities to coordinate web sites and minimize duplication and confusion.

   I. The FileLocal site will include governance, policy, and planning issues.

   II. Cities will include a banner or icon on their websites that links to FileLocal. They will not duplicate or maintain FileLocal information on city websites.

I. Every effort will be made to maintain clear and timely internal communications between FileLocal and its partner cities. This includes, at a minimum, quarterly communication meetings between FileLocal and city communicators and regular reports from the Project Manager to the FileLocal Board.

6. Key Contacts (Reference Appendix B)

FileLocal

Program Manager
PO Box 94669, Seattle, WA 98124
206-233-2513

Principal Cities

City of Bellevue

City of Des Moines

City of Everett

City of Lake Forest Park

City of Renton

City of Seattle

City of Tacoma

7. Conflict Resolution

It is the intent of all parties to act in good faith on all matters. Should a dispute arise between the FileLocal Board, Program Manager, Vendor and/or cities over any of the agreed upon protocols or related to communications, the FileLocal Board Chair and Program Manager will be the main points of contact.

The parties shall seek in good faith to resolve any such dispute or concern by meeting, as soon as feasible. The meeting shall include the Chair of the Executive Board, the Program Manager, and not more than two (2) representatives of the City with positional authority to negotiate and resolve the dispute,

Conflict of Interest Policy

1. Purpose

The purpose of this policy is to establish guidelines for ethical standards of conduct to govern Washington Multi-City Business License and Tax Portal Agency board members, agency staff, and any employees (hereafter referred to as Agency officials) in the performance of Agency business and the duties of their respective jobs. This policy is intended to provide positive direction in order to prevent potential conflicts of interest. This policy is not all encompassing in its definition of conflict of interest. Action deemed inappropriate by a reasonable person, whether specifically cited in this policy or not, shall be subject to inquiry under this policy.

2. Definitions

The following definitions shall apply for purposes of this policy:

A. “Agency official” is any Agency staff, Board member, or employee as defined below.

B. “Agency staff” is any employee provided under a loaned staff agreement.

C. "Board member" or “Executive Board” member is the individual representing a principal on the Executive Board, whether the Chief Financial Officer of such principal or his/her designated alternate.

D. "Business" is any corporation, partnership, sole proprietorship, firm, enterprise, franchise, self- employed individual, consultant, holding company, joint-stock company, receivership, trust, or any legal entity organized for profit.

E. "Employee" is a person or persons employed on a full-time continuing basis by the Agency and, for the purpose of this policy only, and shall include part-time, intermittent, or temporary workers. The term shall not include employees of Seattle who provide services or perform duties for the Agency pursuant to interlocal agreement, loaned staff agreement, between the Agency and Seattle. The term shall not include persons engaged or retained by the Agency pursuant to contract to perform consulting or special technical services.

F. "Gift" is anything of economic value, but shall not include campaign contributions regulated by the provisions of chapter 42.17A RCW, informational materials exclusively for official or office use, memorials, trophies and plaques of no commercial value.

"Immediate family" is an Agency official’s spouse, domestic partner, child or the child of an Agency official’s domestic partner, and other dependent relatives if living in his or her household.

G. "Interest" is any direct or indirect monetary or material benefit accruing to an Agency official as a direct result of contracts or transactions which are or may be the subject of an official act or action by or with the Agency, except contracts or transactions which confer similar benefits to all other persons and/or property similarly situated. An Agency official shall not be deemed to have an interest in conflict with his or her official duties for purposes of this code if the interest is remote

"Remote interest" means:

i. That of a non-salaried officer of a nonprofit corporation;

ii. That of a landlord or tenant of a contracting party; or

iii. That of a creditor, debtor or ownership interest of less than one thousand five hundred dollars in a business entity which is a contracting party or as a holder of less than one percent of the shares of a corporation or cooperative which is a contracting party, whichever is less.

H. "Program Manager" is the chief operating officer for the Portal Agency appointed by and serving at the pleasure of the Executive Board.

3. Background

In keeping with the policies declared by the State Legislature in enacting codes of ethics for municipalities, it is recognized that high moral and ethical standards among public officials and employees are essential to the conduct of government. A code of ethics for the guidance of Agency officials is necessary in order to avoid and prevent conflicts of interest in public office, to improve standards of public service and to promote and strengthen the faith and confidence of the citizens in the Agency. Agency officials are, therefore, obligated to treat their offices and duties as a public trust, using their official powers and duties and the resources of the Agency only to advance the public interest. It is expected that Agency officials will conduct their public and private actions and financial dealings in a manner that will present no actual or apparent conflict of interest between the public trust and their private interests.

This obligation requires that all Agency officials devote their best efforts and attention to:

A. Being independent and impartial in the exercise of their duties and avoiding actions that create even the appearance of using their positions for personal gain or private benefit.

B. Strengthening public confidence in the integrity of the Agency's decisions by demonstrating the highest standards of personal integrity, fairness, honesty, and compliance with both the spirit and the letter of the law and this resolution.

C. Creating a work environment that is free from all forms of unlawful discrimination and harassment.

D. Managing human and environmental resources for the benefit and enjoyment of both current and future generations.

E. Conducting the public's business openly and, to the maximum extent consistent with existing law, resolving doubtful cases in favor of public access.

F. Serving the public with respect, concern, courtesy, and responsiveness, recognizing that service to the public is the primary mission of government.

G. Promoting an environment of public trust free from fraud, abuse of authority and misuse of public property

H. Protecting the integrity of the decision-making process by recognizing and avoiding conflicts between public duties and private interests and activities.

I. Respecting and protecting privileged information to which Agency officials have access in the course of their official duties including, but not limited to, information provided in lawful executive sessions of the Board.

4. Policies and Procedures

A. Gifts

No Agency official shall accept any gifts.

B. Use of Agency Property

No Agency official shall request, use, or permit the use of Agency-owned vehicles, equipment, materials, or property for personal convenience or profit. Use is to be restricted to such services as are available to the public generally and for the conduct of official business.

C. Procurements

I. The Agency intends to conduct its procurements of work and for professional services with integrity, fairness, and openness. Agency officials involved in Agency procurements shall not act or fail to act in any way which compromises the fairness of Agency procurements or which creates actual or apparent conflicts of interest. Agency officials are expected to use good judgment and to act in accordance with Agency policies, policies of the member jurisdiction, applicable laws, and the best interests of the Agency. The Program Manager for the Agency shall be the focal point for receiving and responding to communications from the public, potential bidders or proposers and other government staff and Board members concerning the procurement unless otherwise approved by the Board.

II. Agency officials directly involved in an Agency procurement process shall promptly identify any past or current personal, financial, or business relationship with any firm, or principals associated with a firm, which submits bids or proposals to the Agency. Disclosure shall be made to the Program Manager for the Agency. Determination of the appropriate response, if any, shall be made by the Program Manager of the Agency with advice of legal counsel.

III. In the event a Board member receives information or requests for information from the public, potential bidders or proposers or other government staff concerning a competitively bid contract or a professional services procurement, the Board member shall:

a. Accept the information or inquiry and provide such information to the Board for response; or
b. Decline to discuss the information or to respond to the inquiry or complaint and instead refer the matter to the Agency Program Manager.

IV. Once a request for bids, request for qualifications or request for proposals is issued by the Agency, Agency officials are encouraged to decline meetings or informational exchanges with potential bidders or proposers. Requests for meetings or information should be referred to the Agency Program Manager.

V. If the information or an inquiry received by an Agency official indicates there may have been a violation of applicable laws, regulations, Board policies, member jurisdiction policies, or administrative procedures, the Board member should promptly refer such complaint, information, or inquiry to the Chair for response. Employees should consult with the Program Manager of the Agency. The Chair may direct the issue to the Program Manager of the Agency and/or legal counsel for response.

D. Conflicts of Interest

I. No Agency official shall engage in any act which is in conflict with the performance of his or her official duties for the Agency or knowingly use his or her office or position for personal or immediate family gain or profit.

II. Any Agency official shall be deemed to have a conflict of interest if the Agency official engages in any of the following activities:

a. Has or is seeking to advance or obtain contractual or other business or financial relationships with the Agency.

b. Conducts operations or activities regulated by the Agency.

c. Has interests which may be substantially affected by the Agency official's performance or non-performance of his or her official duties for the Agency.

d. Receives or has any financial interest in any sale or lease to the Agency of services, materials, equipment or property when such financial interest is received with the prior knowledge that the Agency intends to purchase, lease or contract for such services, materials, equipment, or property.

e. Participates in his or her capacity as an Agency official in the making of a contract in which he or she has a private pecuniary interest, direct or indirect, or performs in regard to such a contract some function requiring the exercise of discretion on behalf of the Agency.

f. Influences the Agency's selection of, or its conduct of business with, a corporation, person or firm having business with the Agency if the Agency official has financial interest in or with the corporation, person, or firm.

g. Engages in, accepts private employment from or renders services for private interests when such employment or service is incompatible with the proper discharge of official duties or would tend to impair independence of judgment or action in the performance of official duties for the Agency

h. Appears on behalf of a private person, other than his or herself or an immediate family member or except as a witness under subpoena, before any regulatory governmental agency or court of law in an action or proceeding to which the Agency or an Agency member in an official capacity is a party or accepts a retainer or compensation that is contingent upon a specific action by the

Agency. Discloses or uses, without legal authorization, confidential information concerning the property or affairs of the Agency in such a way as to benefit himself or herself or a member of his or her immediate family with respect to any contract or transaction which is or may be the subject of official action of the Agency.

i. Has a financial or personal interest in any action or decision coming before the Agency and participates in discussion with or gives an official opinion to the Agency unless:

i. The Agency official discloses on the record of the Agency the nature and extent of such interest or makes a good faith effort to comply with the disclosure requirement and procedures included within these policies, and

ii. It is confirmed that a conflict of interest does not exist, or such interest is determined by the Agency to be immaterial.

iii. Takes any action in the course of his or her official duties for the Agency in regard to providing service to specifically benefit the regulation or development of property or of a private business or enterprise in which the Agency official holds an interest in, directly or indirectly, for purposes of personal financial gain, investment or speculation provided, that this prohibition shall not apply to:

iv. Real property devoted to the personal use or residence of the Agency official or a member of the Agency official's immediate family, or

v. Any other interest in real property held by an Agency official on the date of enactment of these policies.

vi. Participates in a transaction involving the appointment, termination of appointment, promotion, demotion, discipline, approval of a salary increase or decrease or the supervision of the work of a member of their immediate family or any other person in whom the Agency official has a financial interest. The conflict of interest prohibitions of this Section shall not apply to activities between a consultant for the Agency or persons employed by or serving as subcontractors.

E. Conduct of Agency Officials

I. Agency officials will conduct themselves according to the rules of conduct below as they pertain to their public service for and on behalf of the Agency.

II. Agency officials shall maintain decorum in meetings and set an example of exemplary conduct when Agency officials represents the Agency. Agency officials shall conduct themselves so as not to bring disgrace or embarrassment upon the Agency.

III. Agency officials shall always represent that opinions stated are the Agency official's own and do not necessarily represent those of the Agency unless the Agency Board has voted and passed a resolution or motion that so states or clearly supports the expressed policy

.

IV. No Agency official shall willfully make any false statement, certificate, mark, rating, or report or in any manner commit any fraud, conceal any wrongdoing or knowingly withhold information about wrongdoing in connection with work-related conduct of any Agency official.

V. Agency officials shall devote their best efforts and attention to maintaining honest, open, and civil communications at all levels of the Agency and with the public.

5. Compliance

A. In order to ensure that the personal and financial interest of Agency officials present no actual or apparent conflicts of interest when any matter in which an Agency official has a personal or financial interest comes before the Agency Board or its standing committees for action or recommendation, the Agency official shall promptly disclose the general nature and extent of such interest on the record of the meeting prior to any discussion or vote on the matter.

B. If a conflict of interest is confirmed through the process described in the next section, the Agency official shall disqualify himself or herself from discussion or voting upon the matter, and shall refrain from discussion or recommendation concerning the matter, if discussion or voting thereon would constitute a conflict of interest, or apparent conflict of interest, as described in this section or violate any other governmental law or regulation.

C. Any Agency official who is disqualified by reason of such conflict of interest shall, after having made the required disclosure set forth above, remove himself or herself from his or her customary seat, or teleconference, during such debate and leave the Board chambers until such time as the matter at hand, from which such Agency official has been disqualified, has been disposed of in the regular course of business. Any action taken by the Board or a committee related to such interest shall be by a vote sufficient for the purpose without counting the vote of the Agency official having the interest.

D. If an Agency official is uncertain whether he or she may have an actual or apparent conflict of interest concerning any matter which is proposed for discussion, action or recommendation by the Agency Board or one of its standing committees, the Agency official shall refrain from communicating with other Board members concerning the matter unless:

I. Such conflict has been disclosed as provided above at a public hearing of the Board or a standing committee and resolved by the chair of the meeting, or

II. Legal counsel of the Agency has been advised of the basis for the questioned actual or apparent conflict and has determined that no conflict of interest as defined by this resolution exists which would either require disclosure or deferral of any discussion, action or recommendation.

E. If during the course of discussion of matters by the Board or a standing committee, a Board member concludes that his or her continued participation may constitute an actual or apparent conflict of interest which was previously unanticipated, he or she shall promptly inquire of the chair of the meeting and Agency legal counsel whether or not disclosure as provided by this section is appropriate or required and proceed as directed by the chair and legal counsel. The discovery and disclosure as provided herein of a previously unanticipated and unintended conflict of interest by a Board member or during his or her discussion of matters pending before the Board or a standing committee shall not disqualify the Board or committee from subsequently taking an action or making a recommendation.

F. If the Program Manager or an employee is uncertain whether he or she may have an actual or apparent conflict of interest they should not make a unilateral decision if there is any doubt, including his/her ability to impartially review a matter involving one's social contact, acquaintance, or friend. The Agency legal counsel should be consulted.

6. Complaints

The Executive Board shall insure the proper implementation of the code of Ethics and will investigate and report on alleged conflicts of interest. The Agency's legal counsel shall be available and shall serve as technical staff for the Board throughout the review process.

A. The Board shall meet within thirty (30) days after receipt of any written complaint.

B. The Board shall render opinions, in writing, concerning questions of ethics, conflicts of interest, and applicability of this Code of Ethics. The Board shall limit its scope to specific complaints and shall not go beyond matters relating to the complaint.

C. The Board shall investigate all formal written complaints, from any source, with regard to alleged violations of this policy if the complaint is determined to be sufficient by legal counsel. The Board may also defer investigation of the complaint to the member jurisdiction for the member who is the subject of the complaint.

D. In the course of its investigation, the Board may require any Board member or the Program Manager or request any other person to appear before the Board to give full information under oath and to produce books, memoranda, papers, documents, financial statements, receipts, canceled checks, or any other relevant information or data in the possession, custody, or control of the person ordered or requested to appear.

E. All witnesses required or requested to attend such hearings shall receive written notification, in person or by certified mail, of the time and place of the hearing at least fifteen days prior to the date fixed for attendance

F. Whenever an Agency official is under investigation for any alleged violation of this Code, he/she shall receive appropriate notice in writing from the Board at least fifteen days prior to any hearing. That Agency official shall also be entitled to be present, to examine and cross-examine witnesses, to be represented by counsel, and to call witnesses on his/her own behalf.

G. In order to protect the rights and reputation of persons who may be unjustly attacked or criticized and given the fact that investigations of complaints may serve as a prelude to further legal or disciplinary action, hearings concerning violations of this Code shall be conducted in private to the extent permitted by state law; provided that, the person subject to the complaint may request that the hearings be conducted in public. A record of such proceeding shall, however, be made and retained.

H. Provided, however, that any Agency official who is the subject of a complaint may demand a public hearing. All hearings whether public or private shall be conducted under the guidelines established herein.

I. The Board shall render a written record of its findings upon conclusion of the investigation.

J. The record of the Board's written findings shall be open to public inspection unless:

i. The information is exempt according to state law (RCW 42.56) and damage to individuals resulting from the release of the record would outweigh the public's need to know;

ii. The Board has determined in the conduct of any hearing or proceeding under its jurisdiction that it is reasonable to withhold information in order to protect individuals who may be unjustly or improperly accused or who may be disproportionately harmed or injured in their reputation, employment, or profession by any premature disclosure;

iii. Civil or criminal action by the Agency or any other governmental agency having jurisdiction may be pending.

7. Remedy

A. If a board member is found to be in violation with these policies, the board may send a letter of admonishment to the member jurisdiction and seek a remedy in accordance with the Agency by-laws.

B. If the Program Manager is found to be in violation he or she will be subject to disciplinary action up to and including termination from employment; provided that, in the event that the Program Manager is a loaned employee, any disciplinary action shall be subject to and implemented in accordance with any agreements in place between the Agency and the employer of the Program Manager.

C. In the event the Board's findings disclose an apparent violation of any state law, a copy of the findings shall be filed with the Prosecuting Attorney of King County.

D. If the Board's findings disclose an apparent violation of any local law, then the Agency's legal counsel may prosecute by appropriate action of either a criminal or civil nature.

E. Any sufficient complaints regarding Agency employees shall be referred to the Program Manager of the Agency, who shall investigate the complaint and take appropriate actio

Emergency Procedures

1. Purpose

To clarify roles and responsibilities in the event of an emergency.

2. Policy

A. FileLocal staff shall follow City of Seattle emergency procedures during the term of the Agreement between FileLocal and the City of Seattle for using City of Seattle office space.

B. Security procedures and roles and responsibilities during an emergency related to the tax portal are described in the service provider agreement between the City of Seattle and e-Gov. These procedures will be reviewed by the Executive Board and will require Executive Board approval. Following approval, the security procedures will be appended to the operating procedures.

C. FileLocal shall have a management group responsible for contingency plans including a line of succession.

3. Responsibility

Program Manager

4. Procedure

A. The Program Manager shall brief the Executive Board on all emergency plans included within the City of Seattle emergency procedures, tax portal service agreement, and communications policies.

B. The Agreement between FileLocal and the City of Seattle provides that the City may backfill a support staff member for a period of less than three consecutive weeks.

C. The line of succession for the Program Manager is as follows: Information Technology Business Analyst (Project Manager).

D. The Executive Board shall establish a line of succession in the event of an emergency that affects personnel in the City of Seattle including the Program Manager and the City of Seattle's Board Member. This succession is as follows: Executive Board Chair; Executive Board Vice-Chair; remaining Executive Board member(s).



FISCAL MANUAL 2.0

DECEMBER 2019
(Updated September 2020)



Fiscal Manual

TABLE OF CONTENTS

Internal Control 2
Accounting Systems 3
Budget 4
Cash Management 5
Cash Receipts and Deposits 6
Local Government Investment Pool 7
Disbursements 8
Revenue and Receivables 15
Procurement and Contract Management 17
Capital Asset Management 19
Journal Entries 21
Financial Reporting 22
Financial Forms 23

1. Internal Control

1.1 Purpose

To ensure that FileLocal assets are received when tendered, protected while in custody, and used only for the purposes intended. To segregate duties and responsibilities so that one person does not handle all phases of a transaction. To establish policies and procedures so that errors, omissions, and irregularities are detected and minimized.

1.2 Policy

Policies and procedures established for the accounting functions shall be designed to achieve and preserve, to the maximum practical extent, internal controls to safeguard the assets of FileLocal, minimize and detect errors and omissions, and maintain an audit trail for independent review of FileLocal's activities.

1.3 Responsibility

Executive Board, Program Manager, the Agency's accounting firm and Others

1.4 Procedure

A. Financial statements and related supporting work prepared by the Agency's accounting staff on behalf of FileLocal shall be reviewed by senior level staff within the Agency's accounting firm.

B. Financial statements prepared by the Agency's accounting firm shall be reviewed by FileLocal's Program Manager on a monthly basis.

C. The Program Manager and Executive Board review, per the resolution authorizing the FileLocal Executive Board meetings for the year, the financial reports, budget variance, and large or unusual transactions.

D. Accounting documents and records shall be maintained in safe, secured drawers and network server at the Agency's accounting firm to prevent their inadvertent or intentional loss.

E. Although not designed exclusively to catch fraud, should our internal control procedures uncover fraud, the Program Manager, the Executive Board, and the State Auditor will be notified within 5 business days.

2. Accounting Systems

2.1 Purpose

To describe the fundamental system for accounting, the internal controls within the financial operation, and the reconciliation between functional areas.

2.2 Policy

Automated and manual accounting systems shall be maintained and reconciled to provide a comprehensive and consistent accounting reporting system that meets federal, state, and local requirements, as well as generally accepted accounting principles.

2.3 Responsibility

The Agency's accounting firm shall establish and maintain a system that ensures that both integrated and independent accounting modules reconcile to the general ledger of FileLocal, and that proper internal controls exist within the various systems to protect the integrity of the data, safeguard the assets of FileLocal, and identify errors and irregularities in the normal course of financial operation.

2.4 Procedure

A. The automated accounting system QuickBooks consists of three components that integrate to produce accurate financial reports and other pertinent information related to the accounting process:

   I. General Ledger

   II. Accounts Receivable

   III. Accounts Payable

B. Capital assets, prepaid expenses and long-term assets and liabilities that are depreciable and amortizable are maintained in Excel spreadsheets. These are designed for FileLocal to keep detailed information to meet the accounting needs of the Agency. Manual systems are reconciled to QuickBooks on a monthly basis.

C. Backup of QuickBooks is performed periodically, at least once a year.. All essential worksheets and other files that are maintained by the Agency's accounting firm are stored on its network server and backed up daily. Records and files are retained at the Agency's accounting firm for seven (7) years.

3. Budget

3.1 Purpose

The biennial budget and related processes provide a tool for achieving financial oversight over the FileLocal's financial well-being. In addition, the budget enables the Program Manager and Executive Board to focus on anticipated revenue, estimated expenditures, capital asset acquisition, long term financial health, and continuity of services.

3.2 Policy

On an annual basis, the Agency will develop and propose a budget for revenue and expenditures for overall program and administration. The budget will be developed, adopted, and administered in accordance with Section 13 of the Interlocal Agreement.

3.3 Responsibility

Executive Board, Program Manager, and the Agency's accounting firm

3.4 Procedure

A. On an annual basis, the Program Manager and the Agency's accounting firm will draft initial revenue and expenditure forecasts. During the annual budget process, the needs of FileLocal are evaluated to ensure proper staffing to meet the needs of the consortium, ensure website data security, and meet the organizational goals. This budget is - in part - established based on the number of customers and emerging community needs.

   a. Reimbursement Allocation: Costs will be allocated to Original Principals and new Participating Cities as follows:

      i. Original Principals – Bellevue, Everett, Tacoma, and Seattle. Allocation will be done using the 2012 actual historical transaction counts through FY 2021. After 2021, the reimbursement allocation will be based on actual transactions processed on the Portal.

      ii. New Participating Cities – The cities' historical counts agreed on during the implementation phase will be used through FY 2021. After 2021, the reimbursement allocation will be based on actual transactions processed on the Portal.

B. The proposed budget is submitted to the Operations Committee for preliminary review and to the Executive Board for its final review and ultimate approval of the budget.

C. Modifications to the budget shall be approved by a supermajority vote of the Executive Board (and also unanimous consent of the Original Principals if required by Section 13 b.iv of the Interlocal Agreement) as necessary from time to time to account for changes in expenditures and revenues.

D. The budget is monitored through a monthly schedule of actual and budget comparisons submitted by the Agency's accounting firm. This schedule shows the variances between year-to-date revenue and expenditures, and amounts budgeted by the Agency.

4. Cash Management

4.1 Purpose

To outline the policy for cash management.

4.2 Policy

FileLocal shall maintain an effective system of cash management that anticipates cash needs and have plans to meet its cash flow needs.

4.3 Responsibility

Program Manager and the Agency's accounting firm

4.4 Procedure

A. All receipts shall be deposited within 3 business days.

B. Disbursements shall be released within 30 days, no later than due date.

C. Every effort will be made to take advantage of early pay discounts if they result in benefit to FileLocal.

D. The Agency's accounting firm shall maintain a current daily balance of checking accounts and shall record deposits and checks in such manner to know the available cash balances at all times.

E. Bank reconciliation is performed by the Agency's accounting firm on a monthly basis and subject to review by the Program Manager.

F. The operating cash reserve goal is to maintain a reserve equal to 15% of the annual budget, consistent with the reserve fund provision in section 13 m. of the Interlocal Agreement.

G. Excess cash shall be invested into the Local Government Investment Pool (LGIP).

5. Cash Receipts and Deposits

5.1 Purpose

To outline cash receipts and deposit policies and procedures.

5.2 Policy

All fees, receipts, and income collected or received are deposited into FileLocal's bank depository account.

5.3 Responsibility

Program Manager and the Agency's accounting firm

5.4 PROCEDURE

A. Cash receipts received by mail at FileLocal Office shall be forwarded to the Agency's accounting firm within 3 business days. Cash receipts received by mail at the Agency's accounting firm are deposited into FileLocal's bank account at Wells Fargo within 3 business days. Checks received must be safekept in a secured drawer.

B. The Agency's accounting firm Administrator opens, sorts, and deposits cash receipts. Deposit slips and copies of checks are given to an accountant at the Agency's accounting firm for booking cash receipts in FileLocal's accounting system.

C. Service fees collected or received by the third-party service company are electronically swiped/transferred to FileLocal's bank account at Wells Fargo. The third-party service company shall provide the Agency's accounting firm daily cash receipts data and documents on a monthly basis.

D. Cash receipt data and documents submitted by the third-party service company are reconciled by the Agency's accounting firm and entered in FileLocal's accounting system. If any errors are encountered, the Agency's accounting firm will notify both the Program Manager and the third-party service company of any overage or shortage. the Agency's accounting firm will contact the third-party service company to obtain the necessary information to make the correction. Once the receipt is correct, the Agency's accounting firm will update the FileLocal general ledger and communicate the corrected data to the Program Manager.

E. Cash receipts are reconciled to bank statements by the Agency's accounting firm on a monthly basis. Monthly bank reconciliation shall be reviewed by the Program Manager.

5.4.1 Local Government Investment Pool

1. Purpose

To outline local government investment pool policies and procedures.

2. Policy

Excess cash shall be invested to the local government investment pool (LGIP). For the purpose of determining the excess cash, excess cash shall be any amount that exceeds $250,000 at the end of the month.

3. Responsibility

Executive Board, Program Manager, and the Agency's accounting firm

4. Procedure

A. The Agency's accounting firm calculates the excess cash on a monthly basis for the purpose of the LGIP investment. The calculation is reviewed by the Program Manager.

B. After any contribution or withdrawal are reviewed and approved by the Program Manager, the Agency's accounting firm follows the LGIP Operation Manual to process the transaction. The minimum contribution or withdrawal shall be $5,000. The minimum amount is required by the LGIP in accordance with WAC 210-01-060.

C. The LGIP paperwork, such as Local Government Investment Pool Authorization Form and TM$ Online Web Access shall be completed by the Program Manager or Treasurer (CEO of the Agency's accounting firm). According to the Resolution No. FL2020-02, the Program Manager and Treasurer are the authorized individuals to authorize all amendments, changes, or alternations to the LGIP documents.

D. The Agency's accounting firm receives the monthly LGIP statement. The Agency's accounting firm conducts a monthly reconciliation. The Program Manager reviews the monthly reconciliation.

E. On a quarterly basis, the Program Manager will present the LGIP activities to the Executive Board for the Board's review.

6. Disbursements

6.1 Authorizations

1. Purpose

To establish signature approval levels for the purpose of authorizing purchases, contracts, and expenditures.

2. Policy

Authorizations for purchases, contracts and all other expenditures excluding the purchase requests made by the Program Manager must follow this delegation of authority

- Unbudgeted authorizations < $5,000 must be approved by the Executive Board Chair and Vice-Chair.
- Unbudgeted authorizations > $5,000 must be approved via a resolution with the Executive Board
- Budgeted authorization < $50,000 must be approved by the Program Manager
- Budgeted authorization > $50,000 must be approved by the Executive Board Chair and Vice-Chair
- All contracts in excess of $5,000 shall be briefed and reviewed with the FileLocal Executive Board at regularly scheduled Executive Board Meeting prior to authorization.

Authorizations for purchases, contracts and all other expenditures requested by the Program Manager must follow this delegation of authority.

- Unbudgeted authorizations < $2,000 must be approved by the Executive Board Chair and Vice-Chair.
- Unbudgeted authorizations > $2,000 must be approved via a resolution with the Executive Board
- Budgeted authorized < $5,000 must be approved by the Treasurer
- Budgeted authorized > $5,000 must be approved by the Treasurer and either the Executive Board Chair or Vice-Chair.
- All contracts in excess of $5,000 must be briefed and reviewed with the FileLocal Executive Board at regularly scheduled Executive Board Meeting prior to authorization.

3. Responsibility

The Program Manager, Executive Board, and the Agency's accounting firm.

4. Procedure

Prior to purchase and/or disbursement all applicable forms and paperwork, including but not limited to Purchase Acquisition Form, must be authorized in accordance with the above policy. See Attachment A for Purchase Acquisition Form.

6.2 Cash Disbursements

1. Purpose

To outline the policy for cash disbursements**.**

2. Policy

Disbursements shall be made only for valid transactions by authorized personnel only.

3. Responsibility

The Program Manager, Executive Board, and the Agency's accounting firm

4. Procedure

A. All disbursements and electronic fund transfers, including ACH transactions, shall be for FileLocal business and each transaction must be supported with properly authorized documentation such as an invoice, payroll record, or expenditure/check request.

B. Invoices and requests for payment must be reviewed and approved by the Program Manager before checks are prepared. Prior to payment, the Agency's accounting firm verifies the authorization of purchase, expenditures, and invoices. A Payment Approval Checklist shall be filled out. See Attachment B for Payment Approval Checklist.

C. The Agency's accounting firm prepares checks and also maintains and initiates electronic payments. Maintenance of vendor information files and initiating of payments will be performed by two separate staff persons at the Agency's accounting firm.

D. Checks made payable to "bearer" or "cash" or signed blank are prohibited.

E. Checks are mailed directly to the payee by the Agency's accounting firm.

F. Checks or electronic payments that are returned or rejected must be investigated and resolved within 2 business days of receipt/notification in order to avert loss from fraud or negligence.

G. Bank statements are received in the mail, reviewed, and reconciled to the general ledger on a monthly basis by the Agency's accounting firm. Copies of checks are to be matched to the supporting documentation. Prior to filing, all disbursement support shall be reviewed for proper documentation and approving signatures. Bank reconciliations and cancelled checks will be available for review by the Program Manager.

A list of vendor names and disbursements is prepared by the Agency's accounting firm and sent to the Executive Board for review on a quarterly basis.

6.3 Check Request

1. Purpose

To outline the policy for check requests.

2. Policy

The Check Request form (see attachment C) must be completed for all expenditures not covered by a Purchase Order Requisition or detailed invoice.

3. Responsibility

The Program Manager shall be responsible for signing check requests to indicate approval. Check and reimbursement request must follow the Authorization Policy in 6.1.2 A&B.

4. Policy Exceptions

A recurring payment does not require a Check Request for the Executive Board or the Program Manager's authorization. These expenditures have been constructively approved by virtue of the Executive Board's approval of the contracts and agreements giving rise to the recurring obligation. A sample list of these types of expenditures is as follows:

A. Purchase orders supported by purchase requisitions;

B. Contract payments supported by previously approved contracts;

C. Pre-authorized temporary personnel help;

D. Contracted labor costs and allocated overhead..

5. Procedures

For the items listed below, no Purchase Order Requisition form is required. A Check Request form may be used: The approval thresholds follow 6.1 Authorizations.

A. US Postal costs;

B. Licenses;

C. Conference fees, tuition, and temporary employment services;

D. Freight bills, express shipping, common carriers, import/export duties, customs & brokerage fees;

E. Travel expenses, including transportation, meals, and hotel;

F. Dues, subscriptions, professional membership & association dues, and

G. Advertising.

6.4 Check Control

1. Purpose

To detail the policy and procedures for control of signed checks and unsigned check stock.

2. Policy

All checks are to be accounted for by check number. the Agency's accounting firm shall maintain internal controls with respect to custody of check stock, preparation, printing, signing, mailing, filing, and voiding of all checks.

3. Responsibility

The Agency's accounting firm

4. Procedure

A. Check stock is to be securely maintained in a locked cabinet at the Agency's accounting firm.

B. the Agency's accounting firm is responsible for typing or printing checks after verifying the approval of payments..

C. Bank reconciliation will include accounting for all void or destroyed checks.

D. All checks will be signed by the authorized check signers – the Program Manager or the Treasurer.

Cancelled checks with bank reconciliation and bank statement prepared by the Agency's accounting firm are forwarded to the Program Manager for review on a monthly basis.

6.5 Travel Expense

1. PURPOSE

To outline the policy for travel expense reimbursement and ensure adequate cost controls are in place, travel expenditures are appropriate and provide a uniform and consistent approach for timely reimbursement of authorized expenses. For the purpose of this policy, Board members are considered staff.

2. POLICY

It is the policy of FileLocal to reimburse staff for reasonable and necessary expenses incurred in connection with approved travel on behalf of FileLocal. FileLocal strongly encourages use of travel discounts when making travel arrangements.

Travelers seeking reimbursement should incur the lowest reasonable travel expenses and exercise care to avoid impropriety or the appearance of impropriety. Reimbursement is only allowed when not available or provided by other sources. If a circumstance arises that is not specifically covered in this travel policy, then the most conservative course of action should be taken.

3. RESPONSIBILITY

Staff travel must be authorized prior to expenditures being incurred. Travelers should verify that planned travel is eligible for reimbursement before making travel arrangements. Within 30 days of completion of a trip, the traveler must submit a check request form and supporting documentation to obtain reimbursement of expenses. The authorization and check requests must follow the same process as outlined in 6.1 Authorizations and 6.3 Check Requests.

4. PROCEDURE

A. Authorized business travel for staff must be pre-approved.

B. Conference registration fees can be pre-paid with a check prepared by the Agency's accounting firm with a completed and approved check request form.

C. Requests for reimbursements of travel-related expenses are submitted via a check request form. This form must be accompanied by supporting documentation and is required to be approved by the Program Manager. Reimbursement requests for the Program Manager must be approved in accordance with 61. Authorizations.

D. The check request form must be submitted to the Agency's accounting firm within 14 calendar days after the trip is completed. Exception approval from the Program Manager or Treasurer is required if this form is not submitted within this timeframe.

E. Reimbursement of travel expenses is based on documentation of reasonable and actual expenses supported by the original itemized receipts. Reimbursements that may be paid by FileLocal are shown below:

Airfare: An original itemized airline receipt, an e-ticket receipt/statement or an Internet receipt/statement is required. The receipt must show the method of payment and indicate that payment was made. Travelers are expected to obtain the lowest available airfare that reasonably meets business travel needs. Travelers are encouraged to book flights at least 20 days in advance to avoid premium pricing. Coach class or economy tickets must be purchased for domestic or international flights. A higher-priced coach ticket cannot be purchased for a subsequent upgrade in seating. First-class tickets are not reimbursable.

Rail Transportation: FileLocal will pay for rail transportation provided the cost does not exceed the cost of the least expensive airfare. An original itemized receipt, original e-ticket receipt/statement or Internet receipt/statement is required. The receipt must show the method of payment and indicate that payment was made.

Automobile (personally owned): A valid driver's license issued within the United States and personal automobile insurance are required for expenses to be reimbursed. Drivers should be aware of the extent of coverage (if any) provided by his or her automobile insurance company for travel that is business or not personal in nature. Reimbursement for use of a personal automobile is based on the mileage rate issued by the Internal Revenue Service. Travelers may opt to request reimbursement for gasoline in lieu of the mileage. In these instances, original itemized receipts are required. A check request form is required for reimbursement for all vehicle-related expenses.

Automobile (rental): Reimbursement for a commercial rental vehicle as a primary mode of transportation is authorized only if the rental vehicle is more economical than any other type of public transportation, or if the destination is not otherwise accessible. Vehicle rental at a destination city is reimbursable. Original receipts are required. When vehicle rentals are necessary, FileLocal encourages travelers to purchase collision damage waiver (CDW) and loss damage waiver (LDW) coverage. FileLocal will reimburse the cost of CDW and LDW coverage; all other insurance reimbursements will be denied. Travelers are required to fill the gas tank before returning the vehicle to the rental agency to avoid service fees and more expensive fuel rates.

Conference Registration Fees: If the conference fee was not prepaid, FileLocal will reimburse these fees, including business-related banquets or meals that are part of the conference registration. Original receipts to support the payment are required. If the conference does not provide a receipt, then a cancelled check, credit card slips/statement or documentation that the amount was paid is required for reimbursement.

Lodging (commercial): The cost of overnight lodging will be reimbursed to the traveler if the authorized travel is 45 miles or more from the traveler's home or primary worksite. The Runzheimer Cost Index will be used for determining the maximum allowable expense for all lodging at the travel destination, with the following exceptions:

a. When the hotel or motel is the conference or convention site, the conference rate is allowable.

b. When the event sponsor arranges the lodging for the event participant, the participant rate is allowable. If the hotel where the event is scheduled in unavailable to the employee, the employee's supervisor may approve lodging expenses at the rate charged at the nearest hotel.

c. Allowable lodging expenses include the cost of lodging and any applicable sales taxes and/or hotel/motel taxes. The original, detailed lodging receipt must be submitted with the expense claim.

d. If reserved rooms are not needed, it is the traveling employee's responsibility to make sure the room is canceled

Meal: FileLocal will pay a per diem amount for meals based on the Runzheimer Cost Index for meals by location. These meal per diem amounts include tips.

a. The amount of authorized meal allowance is determined on a per meal basis dependent upon the departure time from Seattle and the arrival time on return to Seattle. Snacks and/or meals served on the airlines will not reduce the meal allowance.

b. If meals are included in a lodging, conference or training registration fee, the employee's daily per diem will be adjusted accordingly. A "continental" breakfast provided at a meeting, conference or training session will not reduce the employee's meal allowance.

c. Reimbursement of meal expenses will be based on actual expenses per meal, limited to the allowable maximum established by the Runzheimer Cost Index. Employees are required to collect original meal receipts for all allowable expenses incurred and to submit those receipts with their expense report.

Parking: Original receipts are required for parking fees, including airport parking. The lodging bill can be used as a receipt when charges are included as part of the overnight stay.

Other Travel Expenses: Other travel expenses, including faxes, photocopies, internet charges, data ports and business telephone calls incurred while traveling, can be reimbursed. Original itemized receipts are required.

The following items that may be associated with business travel will not be reimbursed by FileLocal:

a. Airline club membership

b. Airline upgrades

c. Business class for domestic flights or first class for all flights

d. Childcare, babysitting, house-sitting, or pet-sitting/kennel charges

e. Commuting between home and the primary work location

f. Costs incurred by traveler's failure to cancel travel or hotel reservations in a timely fashion

g. Evening or formal wear expenses

h. Haircuts and personal grooming

i. Laundry and dry cleaning

j. Personal entertainment expenses, including in-flight movies, headsets, health club facilities, hotel pay-per-view movies, in-theater movies, social activities, and related incidental costs

k. Travel accident insurance premiums or purchase of additional travel insurance

l. Other expenses nor directly related to the business travel

7. Revenue and Receivables

7.1 Revenue Recognition

1. Purpose

To establish revenue recognition policy and procedures.

2. Policy

All revenue is recognized in accordance with generally accepted accounting principles.

3. Responsibility

Executive Board, Program Manager, and the Agency's accounting firm

4. Procedure

A. Current revenue consists of service fees, reimbursable costs, and shared cost reimbursement from participating cities of FileLocal.

B. Service fees are recognized at the time a customer completes his or her licensing application. Cash basis might be used for the monthly financial reporting; however, service fees would be accrued under GAAP (generally accepted accounting principles) on the annual financial statements.

C. Reimbursable costs are pre-determined through budget, subscriber agreement or inter-local agreement, including any amendments. Reimbursable costs are billed at the beginning of the year and recognized as revenue at that time. On an annual basis, actual costs to be reimbursed are compared to amounts budgeted and billed. Adjustments will be made to reconcile billed reimbursable costs to accrual amount of costs incurred. Credits might be issued to the participating cities when an overbilled amount is identified; and as a result, a reduction of revenue is recognized. If additional costs are identified to be reimbursed from the participating cities, additional invoices are submitted to the participating cities. Additional reimbursable costs are also recognized when billed.

D. For cities which join FileLocal during the year, the reimbursable costs will be billed based on the go live date.

E. Any other contributions and donations are recognized as revenue when cash is received.

F. Any changes in revenue recognition shall be made in writing by the Program Manager and/or the Agency's accounting firm and is subject to approval by the Executive Board.

7.2 Billings and Accounts Receivable

1. Purpose

To ensure billings are made for services actually provided and based on the Interlocal Agreement, subscriber agreement or budget.

2. Policy

FileLocal shall follow prudent and efficient business practices to obtain payment of its receivables.

3. Responsibility

Executive Board, Program Manager, and the Agency's accounting firm

4. Procedure

A. Service fees are paid by customers when they submit their licensing applications. Automatic billing and payment processing are done daily by the third-party service company. the Agency's accounting firm performs a monthly reconciliation of service fees and cash receipts. The monthly reconciliation is forwarded to the Program Manager for review.

B. the Agency's accounting firm prepares invoices for reimbursable cost revenue based on the budgeted amount established at the beginning of the year and/or the prorate share of new cities. At year-end, the Agency's accounting firm conducts a reconciliation of reimbursables according to the actual operation revenue. Any refund or under-billed amounts identified by the Agency's accounting firm through the annual reconciliation is subject to review and approval by the Program Manager and then the Executive Board. Refunds or additional invoices are then processed by the Agency's accounting firm.

C. On a monthly basis, Accounts Receivable is reconciled by the Agency's accounting firm. For any delinquent balance, the Agency's accounting firm sends letters requesting payment and makes a reasonable effort via other means to contact and collect outstanding balances. Monthly Accounts Receivable aging reporting is included in the monthly financial statement packet for the Program Manager and the Executive Board's review.

D. Any adjustments and write-off to Accounts Receivable (excluding purely accounting adjustments/corrections) is subject to approval by the Program Manager. Any the write-off amount in excess of $2,000 is also subject to approval by the Executive Board.

E. All payments received by the Agency's accounting firm are reconciled to Accounts Receivable, the general ledger, and the bank deposits (part of monthly bank reconciliation).

8. Procurement and Contract Management

8.1 Procurement

1. Purpose

To outline procurement policies and processes.

2. Policy

All contracts for labor, professional services, lease of equipment, and supplies for $10,000 or more must be let by free and open competitive bidding, on sealed bids, to the responsible bidder.

3. Responsibility

Executive Board and Program Manager

4. Procedure

A. FileLocal is required to advertise for sealed bids on contracts for labor, professional services, and equipment leases in excess of $10,000 by posting a notice at its website or by publication of a one-time notice in a newspaper published in the State of Washington.

B. In case of an emergency affecting the public's health, safety, economic welfare, or security, a contract may be let to the extent necessary to meet the emergency without public advertisement. The Program Manager will honor payment for a period of six months from the date of declaration posting; should the emergency continue to exist after a six-month period, it will be necessary to re-declare the emergency.

C. Sealed bids are accepted by the Program Manager for evaluation. Based on the Program Manager's recommendation, the Executive Board approves and awards the responsible bidder through competitive bidding with consideration given for the quality of the commodities, conformity to specifications, terms of delivery, and freight charges. Multiple awards may be issued, if notice is contained within the competitive bid, when technical compatibility and/or operational specification are required.

D. A contract for labor, professional services and equipment leases will be let for periods no greater than five years.

E. An awarded contract is not assignable by the bidder without written consent of FileLocal. A contract cannot be assigned to a bidder whose bid was rejected.

8.2 CONTRACTS

1. PURPOSE

To provide policy and procedures for the review, approval, establishment, and modification of personal and professional services contract.

2. POLICY

All contracts should be authorized according to the Authorization Policy and approved as to form by the Agency's attorney.

3. RESPONSIBILITY

Executive Board and Program Manager

4. PROCEDURE

A. Personal and professional service contracts must include the following information:

   I. Name, including contract name and tax identification number (Form W-9);

   II. Scope of contract – what is to be done, the purpose, goal, job, etc.;

   III. Term of contract, including the beginning and ending dates;

   IV. Total contract amount and the method of payment;

   V. Termination clause;

   VI. Signatures.

B. A contract cannot be assigned to a third party. If a different contractor is required, the original contract must be canceled, and a new contact must be initiated.

C. An emergency contract for personal or professional services shall be let for a period of not more than 6 months.

D. Contracts between governmental entities must be separately tracked to ensure additional reporting and regulatory compliance required by federal and state law.

9. Capital Asset Management

9.1 Capitalization Policy

1. Purpose

To define capitalization policy.

2. Policy

All personal and real property with an initial individual cost of more than $5,000 and an estimated useful life in excess of two years are recognized as capital assets. Such assets are recorded at historical cost. Donated capital assets are recorded at acquisition value at the date of donation. Costs for additions or improvements to capital assets are capitalized when they increase the effectiveness or efficiency of the assets. The costs for normal maintenance and repairs are not capitalized. Capital assets are depreciated using the straight-line method over the following estimated useful lives:

- Software 3 – 5 years
- Computers and equipment 3 – 7 years

3. Responsibility

Program Manager and the Agency's accounting firm

4. Procedure

A. The Agency's accounting firm shall assign the appropriate accounting classification codes to all purchases, contracts and acquisitions that qualify as capital assets.

B. The Program Manager shall provide the Agency's accounting firm copies of all purchase orders, requisitions, and receiver's reports covering capital asset purchases.

C. The Agency's accounting firm shall be responsible for recording the asset on the capital asset schedule, a manual spreadsheet/sub-ledger, showing the description, physical location, owners, cost, acquisition date, useful life, depreciation, and disposition date including the date of disposal and sales price of the property.

9.2 Physical Inventory

1. Purpose

To establish physical inventory of capital assets

2. Policy

All capital assets should be inventoried periodically, but not less than every two years, to reconcile the total capital assets with the capital asset schedule (a sub-ledger).

3. Responsibility

Program Manager and the Agency's accounting firm

4. PROCEDURE

A. The Agency's accounting firm shall perform a physical inventory of capital assets at least once every two years.

B. Once the physical inventory is complete, it must be reconciled to the individual capital asset record (a manual capital asset sub-ledger) and general ledger.

C. Inventory count sheet and reconciliation is subject to the Program Manager's review. Any discrepancy is investigated by the Program Manager.

9.3 DISPOSITION

1. PURPOSE

To outline disposition of capital assets.

2. POLICY

All capital asset dispositions shall be approved by the Program Manager. Any disposition in excess of $10,000 shall be approved by the Executive Board.

3. RESPONSIBILITY

Program Manager and the Agency's accounting firm

4. PROCEDURE

A. Disposition of capital assets shall be requested in writing and addressed to the Program Manager. Any disposition in excess of $10,000 shall be approved by the Executive Board.

B. All disposition documents shall be forwarded to the Agency's accounting firm to record the disposition. Gains and losses are recognized on the sale of capital assets.

C. The capital assets and related depreciation shall be removed from both the capital asset sub-ledger and general ledger.

9.4 CAPITAL ASSET IMPAIRMENT

1. PURPOSE

To outline capital asset impairment policy and procedures.

2. POLICY

Capital asset impairment is conducted on an annual basis or at the time the impairment occurs. Only permanent impairments of capital assets should be recognized in the financial statements.

3. RESPONSIBILITY

Program Manager and the Agency's accounting firm

4. PROCEDURE

A. The Agency's accounting firm shall conduct an impairment analysis on an annual basis, or at time the impairment occurs in accordance with the generally accepted accounting principles.

B. A memo of impairment analysis with calculated loss prepared by the Agency's accounting firm is submitted to the Program Manager for review and approval.

C. The Agency's accounting firm records impairment losses in FileLocal general ledger system.

10. Journal Entries

1. PURPOSE

To outline types of journal entries and internal controls over journal entries.

2. POLICY

All journal entries must be self-balancing and include an account type (asset, liability, revenue, expense, net assets) for each line of the journal entry. Journal entries are subject to review and approval based on the policies and procedures herein.

3. RESPONSIBILITY

Program Manager and the Agency's accounting firm

4. PROCEDURE

Journal entries are used to:

A. Correct errors: most of journal entries will be to correct account-coding errors. The journal entry must include the debit entries and credit entries to correctly produce the required accounting effects. There is no review or approval required for this type of journal entry prior to or after posting the journal entries.

B. Record cost allocation: cost allocation is processed by the Agency's accounting firm based on the approved cost allocation documents, including budgets. No review or approval is required for this type of journal entry.

C. Record recurring balance sheet transactions: recurring journal entries include monthly depreciation, amortization, receivable, and accrued liabilities. They are not required for review or approval.

D. Journal entries for month-end and year-end closing, such as accruals, are subject to internal controls within the Agency's accounting firm following GAAP. There is no review or approval required prior to or after posting the journal entries.

E. Implement accounting policies and guidance: a memo is prepared for the implementation of a new accounting standard by the Agency's accounting firm to the Program Manager for review and approval. The memo will provide a reference of the new accounting standard, accounting effects, and a proposed journal entry

F. Record non-routine, nonrecurring transactions: a memo in writing to the Program Manager is required for review and approval of non-routine, non-recurring transactions.

11. Financial Reporting

1. PURPOSE

To establish and catalog the reporting requirements for accounting.

2. POLICY

Financial statements and reports shall be prepared on a monthly and annual basis to provide the Program Manager and Executive Board, and outside auditors with sufficient financial information to report accurately the results of operations.

3. RESPONSIBILITY

The Agency's accounting firm shall maintain supporting records in sufficient detail to prepare financial statements or reports for FileLocal.

4. PROCEDURE

A. On an annual basis, Francis and Company prepares and presents:

I. Annual financial statements with full footnote disclosures,

II. Other required supplemental schedules and information.

The annual financial statements are prepared in accordance with generally accepted accounting principles. The annual financial statements along with required supplemental information are subject to review by the Executive Board and the Program Manager. The Executive Board adopts the annual financial statements.

B. On a quarterly basis, the Agency's accounting firm submits to the Executive Board to adopt:

I. List of vendor warrants.

C. On a monthly basis, the Agency's accounting firm prepares and presents:

I. Internal financial statements (currently using cash basis).

II. Schedule of actual and budget comparison.

III. Variance analysis, as needed, will be prepared with monthly financial statements.

Attachment A Purchase Requisition Form

FileLocal

Purchase Acquisition Form

Requested by:		Date:	
Purpose or Use:			
Vendor Name:			
Vendor Address:			
Vendor Contact:		Phone:	

Product/Service Description	Qty	Unit Price	Extended Cost
Approvals:		Date:	
Approvals:		Date:	

Attachment B Payment Approval Checklist

FileLocal

Payment Approval Checklist

We are required to fill out this payment approval checklist prior to processing a check payment for FileLocal. A check must be processed once the proper approval is verified through this checklist. Once this checklist is filled out and a check is processed, this checklist shall be forward to FileLocal for record.

	YES	NO	N/A
Is Purchase Acquisition Form or Check Request Form attached to an invoice/itemized receipt for processing payment? (Please Note Purchase Acquisition Form or Check Request Form is not required for a recurring payment.)			
Is Purchase Acquisition Form or Check Request Form approved by authorized person (s) in accordance with 6.1 Authorizations of Fiscal Manual? For a recurring payment, is vendor's invoice/itemized receipt approved in accordance with 6.1 Authorization of Fiscal Manual?			
Is vendor's invoice reviewed for GL coding and recording?			

Preparer:	
Date:	

Attachment C: Check Request Form

FileLocal
Check Request Form

Deliver Check to:

Date Required	Check Amount

Purpose of Payment

G/L Account #:

Vendor Name	Invoice/Receipt Number	Invoice Date	Amount

Originator	Date

Approval	Date



Information Technology Securities Policy Manual

TABLE OF CONTENTS

POL-001: Information Management 2

POL-010: Information Classification 6

POL-015: Personnel Security 9

POL-020: Access Control 11

POL-030: Encryption 14

POL-040: Infrastructure 16

POL-050: Physical and Environmental 19

POL-060: Third Party Management and Outsourced Services 21

POL-070: Data Backup 24

POL-080: Data Storage Media Library Management 27

POL-090: Compliance 30

POL-100: Incident Response 34

POL-110: Security Risk Assessment 37

POL-130: System Development Life Cycle 39

POL-140: Business Continuity 41

GDE-200: Guidelines for Information Owners and Custodians 43

Information Management (POL-001)

1. Purpose

The Information Management Policy defines the principles to be used in the protection of the agency's assets from all threats, whether deliberate or accidental, with the objective of ensuring business continuity, protecting employees and participating cities and minimizing the impact of security breaches.

The purpose of this policy is to:

A. Create an environment within the Washington Multi-City Business License and Tax Portal Agency (dba FileLocal) that protects the confidentiality, integrityand availability of information:

- Confidentiality: ensuring that information is accessible only to those authorized to have access
- Integrity: safeguarding the accuracy and completeness of information and processing methods
- Availability: ensuring that authorized users have access to information and associated assets when required

B. Set a uniform framework of policies by establishing principles that are to be applied throughout FileLocal in the management of information.

C. Support the selection of physical, technical and administrative security controls, which are cost-effective, prudent and operationally efficient.

D. Support the oversight functions necessary to ensure compliance with external security requirements.

E. Inform staff, vendors and participating cities of their accountability for protecting FileLocal information resources.

F. Ensure the vendors and participating cities protect FileLocal information processing operations from incidents of hardware, software or network failure resulting from carelessness, intentional abuse or accidental misuse of the system.

G. Enable management to be prepared for prudent action in the event of compromise of any security system or disaster.

2. Underlying Philosophy

This policy was written using the following rationale/philosophy:

A. FileLocal has a duty to protect its staff, information, information technology (IT) and intellectual property and an obligation to ensure vendors and participating cities provide a secure environment for employees and members of the public who have begun the process of becoming a FileLocal client.

B. Well-defined and implemented information policies and standards enable FileLocal to create secure operating environments by balancing controls and risks.

C. The level of security provided will be in line with the threat or risk and will meet the appropriate statutory and regulatory requirements.

D. Employees, and those undertaking work on behalf of FileLocal, are responsible for maintaining security over all aspects of their work and for ensuring that assets, resources and information entrusted to them are protected effectively.

E. Agency staff are expected to observe FileLocal's Code of Ethics.

F. Security is the management's accountability but the responsibility of all staff, participating cities, vendors and contractors. FileLocal understands both vendors and participating cities will have their own Information Security policies and those policies should be in alignment with the policies below and in many cases maybe more than what is needed for FileLocal.

G. Information security is:

- A cornerstone of maintaining public trust
- A business concern — not a technology issue
- Risk-based and cost-effective
- Aligned with FileLocal business strategy

3. Scope

This policy applies to:

A. All FileLocal agency staff (including, but not limited to, permanent employees, contractors, temporary staff, etc.) that have access to the FileLocal service

B. Vendors and service providers (including but not limited to, permanent employees, contractors, temporary staff, etc.) responsible for the Tax Portal and Tax Payment systems which make up the FileLocal service

C. FileLocal participating cities (including but not limited to, permanent employees, contractors, temporary staff, etc.) developing and maintaining back-end data connections to the FileLocal service

D. All data and information regardless of processing mode (e.g. manual or computer) and storage mode (including but not limited to electronic or hard copy form).

E. All technologies associated with the creation, collection, processing, storage, transmission, analysis, and disposal of information

F. All data processing activities performed within or on behalf of FileLocal (including but not limited to all subsidiaries, etc.).

G. All facilities regardless of processing mode (including but not limited to batch, remote and data communication).

4. Policy Statements

A. FileLocal recognizes the immense value and importance of its staff, assets, information, and IT and is committed to ensuring their continued protection.

B. FileLocal shall seek to ensure vendors and participating cities follow IT security policies in order to protect its staff, assets, information, and information technology assets at a level appropriate to the prevailing security threat, with standards and best practice defining the minimum level of achievement.

C. Information Management shall be a consideration at the design and development stages of every business activity and not merely during implementation.

D. FileLocal shall seek to ensure vendors and participating cities make continuous improvement in methods of threat analysis and information management so that it can protect itself appropriately.

E. This policy document shall be approved by the FileLocal Executive Board, published and communicated, as appropriate, to all agency staff, vendors and participating cities.

F. This policy shall be reviewed annually, and in case of influencing changes, to ensure it remains appropriate.

G. FileLocal Information Management Policy shall comply with the FileLocal Information Management Framework and conform to ISO 17799:2005: Information Technology – Security Techniques – Code of Practice for Information Security Management. Cities can elect to use other IT Policies based on proven and adopted Federal Security standards provided those policies still meet the information management and framework adopted bythe Agency

5. Enforcement

Failure to comply with terms and conditions of the FileLocal Information Management Policy may lead to disciplinary action being taken against the individual and in some cases could result in legal proceedings. Any failure to comply with terms and conditions from a participating city could also result in a City no longer being able to use FileLocal.

6. Roles and Responsibilities

A. FileLocal

The agency is responsible for:

- Ensuring that Information Management policy is integrated into all related business operations and that information management activities are coordinated acrossthe same.
- Awareness of the company's information risk profile and ensuring that information risks are mitigated to an acceptable level in accordance with this policy.
- Ensuring that the information management strategic objectives are in alignment with the business strategy.

B. FileLocal Attorney

Chief Counsel is responsible for:

- Review of policies

C. FileLocal Executive with Information Security responsibilities

The Chief Information Security Officer (CISO) or designee, or in lieu of a dedicated CISO, the member of FileLocal who is ultimately responsible for information security, is responsible for:

- Development and maintenance of this policy
- Development of information security principles and practices.
-

- Development and maintenance of the more detailed FileLocal IT information security policy control framework.
- Monitoring the effectiveness of information security across staff, vendors and participating cities.
- Providing the Agency with policy compliance status to statutory and regulatory requirements.

D. FileLocal Agency Staff

FileLocal is responsible for:

- Maintaining security over all aspects of their work and for ensuring that assets, resources and information entrusted to them are managed properly.
- Complying with all information management policies and procedures.
- Reporting all known or suspected security weaknesses and breaches to their line manager or the relevant security manager.

E. Vendors

Vendors are responsible for:

- Maintaining security over all aspects of their work and for ensuring that assets, resources and information entrusted to them are managed properly.
- Complying with all information management policies and procedures.
- Reporting all known or suspected security weaknesses and breaches to their line manager or the relevant security manager.
- Ensuring implementation of Information Management policies, principles and practices throughout the FileLocal service and with vendor staff

F. Participating Cities

Participating cities are responsible for:

- Maintaining security over all aspects of their work and for ensuring that assets, resources and information entrusted to them are managed properly.
- Complying with all information management policies and procedures adopted by a City's CISO, or designee,
- Reporting all known or suspected security weaknesses and breaches to FileLocal if those areas affect the connections between a city's system of record and FileLocal.
- Ensuring implementation of Information Management policies, principles and practices throughout the city staff responsible for the connections between the City system of record and FileLocal.

Information Classification Policy (POL-010)

1. Introduction

Companies process, use, and manage enormous amounts of information. Such information covers the spectrum of sensitivity, in terms of being highly valuable or less valuable, to the company and its customers. To bring a focus to protecting that which is valuable, a classification schema for information is necessary. A classification schema allows security to be directed and invested where that effort is most needed to protect the business environment. Without a classification schema, much effort would be wasted to protect information that is not cost or security justified. A classification schema should also provide both guidance to staff and the tools to apply the right level of classification to information to bring a balance of investment and attention to the overall protection responsibility.

2. Purpose

The purpose of this policy is to allow information, in its many forms, to be classified according to its degree of sensitivity and thus allow the appropriate controls to be applied to ensure its protection.

3. Scope

The Information Classification Policy applies to those who utilize the FileLocal Tax Portal owned by the Washington Multi-City Business License and Tax Portal Agency (FileLocal):

- Agency staff
- Temporary supplemental staff
- Contractors
- Vendors
- Consultants
- Participating cities
- All business partners and parties
- FileLocal system users

The Information Classification Policy also applies to all information systems, data, business applications and networks, used or administered by FileLocal and to all computational environments operated by, or operated on behalf of FileLocal.

Deviation from this policy is acceptable only if an information security threat and risk assessment has been completed with a documented business impact analysis and the Information Owner(s) have signed a risk acceptance form. The Risk Acceptance Form shall be authenticated by the Program Manager.

4. Policy Statements

A. All information shall have a designated Information Owner.

B. Information classification shall adhere to the classification scheme and guidance defined in this policy.

C. Information assets shall be classified according to:

1. Confidentiality
2. Availability
3. Integrity requirements
4. Business Impact of unauthorized disclosure

A. Information Owners shall be responsible to classify the information, whose ownership has been assigned to them.

B. Users shall be responsible to manage information relative to its classification level.

C. Information shall be labelled and safeguarded relative to its classification level

D. Information labelling shall apply to information assets in physical and electronic forms

E. Information managed within FileLocal shall be classified relative to the following hierarchy and aligns to classifications adopted at a local and State level:

1. PUBLIC
2. SENSITIVE
3. CONFIDENTIAL
4. CONFIDENTIAL, WITH SPECIAL HANDLING
5. CONFIDENTIAL' classification shall be the default classification.

D. Information shall be handled in accordance with the requirements set forth in the 'Information and Media Handling Standard'.

E. Information shall be retained in accordance with the requirements set forth in the 'Information Retention Standard'.

F. Information shall be destroyed once the applicable retention period has been exceeded.

G. Information shall be classified at the level of the highest component part. (For example, a document of fifty pages containing one page of 'CONFIDENTIAL' information shall be classified as 'CONFIDENTIAL').

H. The classification level of information shall be reviewed annually. Impact assessments shall be undertaken and / or reviewed for critical systems, or those holding 'CONFIDENTIAL' annually.

I. Information resources (i.e. systems, devices, applications) shall implement controls to be compliant with the requirements of the highest classification level of the information that it stores, processes, or transmits.

5. Roles and Responsibilities

1. PROGRAM MANAGER

The Program Manager is responsible for:

- Performing organizational self-assessment periodically to ensure compliance with this policy and related standard.
- Leading the investigation of any reported breaches in FileLocal environment in regard to inappropriate information handling.
- Ensuring that all employees are trained in regard to the applied information handling controls,

2. FILELOCAL AGENCY STAFF

FileLocal is responsible for:

- Assigning the classification category to the information, whose ownership has been assigned to the Agency.
- Maintaining an inventory of their business information for which they are responsible.
- Reviewing annually the classification level of the information for which they are responsible.
- Seeking to ensure controls are applied to their information resources, according to the resource classification category by the appropriate vendors and participating cities
- Ensuring proper management of information for which they are responsible by ensuring information retention requirements are being met by the appropriate vendors and participating cities
- Reporting information security compromises to the CISO, or designee, when inappropriate handling of information has occurred.

3. VENDORS

Vendors are responsible for:

- Assisting Information Owners to implement and manage those controls mandated by the Information Classification Policy and related artifacts.
- Assisting the Program Manager, or their designee's organizational self-assessment initiatives to confirm information classification and handling methods used, adhered to, and are implemented in accordance with this policy and related artifacts.
- Monitoring compliance to confirm currency and effectiveness of this policy and related artifacts.
- Identifying inappropriate usage of information, and the reporting thereof as incidents to the CISO, or designee.
- Assisting the Program Manager, or their designee, in investigations in regard to inappropriate handling of information.

4. PARTICIPATING CITIES

Participating Cities are responsible for:

- Assisting Information Owners to implement and manage those controls mandated by the Information Classification Policy and related artifacts as adopted by their CISO, or designee.
- Assisting the FileLocal Program Manager, or designee's, organizational self-assessment initiatives to confirm information classification and handling methods used, adhered to, and are implemented in accordance with this policy and related artifacts.
- Monitoring compliance to confirm currency and effectiveness of this policy and related artifacts.
- Identifying inappropriate usage of information, and the reporting thereof as incidents to the FileLocal Program Manager, or designee, and to a City's CISO, or designee.
- Assisting the FileLocal Program Manager, or designee, in investigations in regard to inappropriate handling of information.
- Promptly reporting violations of this policy and related standard to FileLocal Agency.
- Understanding the Information Classification Policy and related artifacts as adopted by a City CISO, or designee, and FileLocal.

6. Compliance

The Information Classification Policy uses and assimilates the following bodies of recognized knowledge: ISO 27002:2013:

- Section 8.1.1 – Inventory of Assets
- Section 8.1.2 – Ownership of Assets
- Section 8.2.1 – Classification Guidelines
- Section 8.2.2 – Labeling of information
- Section 8.2.3 – Handling of information
- Section 8.3.2 – Disposal of Media
- Section 8.3.3 – Physical Media Transfer
- Section 13.2.3 – Electronic Messaging
- Section 10 – Cryptography
- Section 18.1 – Compliance with Legal and Contractual Requirements

7. Related Documents

- Information and Media Handling Standard
- Information Retention Standard

Personnel Security Policy (POL-010)

1. Introduction

Secure operations of applications and systems requires the employment of trusted personnel for administration of applications, systems, and data. Appropriate personnel must be hired, and employees must be properly educated regarding their specific information security responsibilities.

2. Purpose

The purpose of this policy is to outline personnel security requirements in order to ensure secure operations by FileLocal.

3. Scope

The Personnel Security Policy applies to all FileLocal employees, as well as any temporary contractors., and all vendors utilized by FileLocal.

Deviation from this policy is acceptable only if an information security threat and risk assessment has been completed with a documented business impact analysis and the Information Owner(s) have signed a risk acceptance form. The Risk Acceptance Form shall be authenticated by the Program Manager.

4. Policy Statements

A. When hiring employees for key technical positions, comprehensive pre-employment screening must take place

B. All pre-employment inquiries must be conducted in full compliance with all FileLocal and/or vendor departmental policies and in full compliance with all related state and federal laws

C. New employees must be informed about their responsibilities and the policies that apply

D. FileLocal must develop formal processes to for disciplinary actions against FileLocal employees who do not follow the requirements documented in FileLocal's information security policies and procedures

E. All employees are required to complete yearly training on the basic tenets of this information security policy

F. All physical and logical access to computing and network facilities and resources must be assigned with the principles of least privilege and separation of duties applied.

G. FileLocal must establish processes to quickly update, close, and/or remove all system and network privileges following the termination or significant change in responsibilities and privileges for any FileLocal employees.

H. Related procedures regarding employee suspension, leave of absence, long term illness or disability must also be established and maintained

5. Roles and Responsibilities

A. PROGRAM MANAGER

The Program Manager is responsible for:

- Performing organizational self-assessment periodically to ensure compliance with this policy and any related standards and/or procedures.
- Leading the investigation of any reported incidents in FileLocal's environment in regard to inappropriate personnel security.
- Ensuring that all employees are trained in regard to appropriate personnel security controls,

B. FILELOCAL AGENCY STAFF

FileLocal agency staff are responsible for:

- Complying with FileLocal requirements regarding personnel security
- Reporting information security compromises to the Program Manager, or their designee, when potentially inappropriate personnel security has occurred.

C. VENDORS (INCLUDING AVENU AND KUBRA)

Vendors are responsible for:

- Implementing security controls that are mandated by this policy and related standards, for the systems of which they are in charge.
- Identifying personnel security incidents, and reporting them to FileLocal and the Program Manager, or designee.
- Assisting the Program Manager, or designee, in investigations in regard to personnel security incidents.
- Providing periodic reports to FileLocal and the Program Manager, or designee, regarding personnel security

6. Compliance

The Personnel Security Policy uses and assimilates the following bodies of recognized knowledge: ISO 27002:2013:

- Section 6.1.1 - Information security roles and responsibilities
- Section 7.1 – Prior to employment
- Section 7.1.1 – Screening
- Section 7.2.1 – Management Responsibilities
- Section 7.2.2 – Information security awareness, education and training
- Section 7.2.3 – Disciplinary process

- Section 7.3.1 – Termination or change of employment responsibilities

7. Related Documents

- N/A

Access Control Policy

1. Introduction

Users need to access data and information resources to be able to perform their daily job functions. Excessive or uncontrolled access can lead to unauthorized or unintentional disclosure and modification of business-critical information. Access to information resources should be granted to those individuals who need that particular information resource to perform their duties.

Access control must balance the restrictions to prevent unauthorized access against the need to provide unhindered access to meet business needs.

2. Purpose

The purpose of the Access Control Policy is to ensure that only authorized users access the Washington Multi-City Business License and Tax Portal Agency (FileLocal) information resources for appropriate business activities.

3. Scope

The Access Control Policy applies to those who utilize information systems, business applications, networks and information owned by FileLocal:

- Agency staff
- Temporary supplemental staff
- Contractors
- Vendors
- Consultants
- Participating cities
- All business partners and parties
- FileLocal system users

The Access Control Policy also applies to all information systems, data, business applications and networks, used or administered by FileLocal and to all computational environments operated by, or operated on behalf of FileLocal.

Deviation from this policy is acceptable only if an information security threat and risk assessment has been completed with a documented business impact analysis and FileLocal has signed a risk acceptance form. The Risk Acceptance Form shall be authenticated by the Program Manager.

4. Policy Statements

A. FileLocal shall prohibit unauthorized access, disclosure, duplication, accidental or unauthorized modification, destruction, misuse or theft of its information.

B. FileLocal shall manage access to information in its computational environment by means of an identification and authentication mechanism.

C. The data, system, application and network access assigned to each user shall be controlled on the basis of business requirements.

D. Member cities shall be authorized by FileLocal prior to being granted access to a particular resource.

E. Users shall only access resources to which they have been granted access.

F. The access control method shall be in accordance with the classification of the resource and the level of risk associated with the resource.

G. All user accounts must be based on unique identifiers that are tied to a specific person. Use of shared accounts is not allowed except when specifically authorized as a documented exception by the owner of the system in question.

H. All administrative access and access to critical/sensitive servers must be secured using multi-factor authentication.

I. User access rights shall be reviewed regularly and modified, revoked, or deactivated as appropriate.

J. User access activities shall be continuously monitored and verified regularly to detect unauthorized

K. access in a timely manner.

L. Creating and assigning access rights to users shall adhere to the following principles:

- Segregation of duties: a principle that prevents the same person from being responsible for the entire transaction end- to-end in an information system. This is done to prevent fraud and abuse of information systems.
- Least Privilege: a principle that ensures that users are granted the most restrictive set of privileges needed to perform their tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use (as opposed to granting users with widely scoped functional privileges that might grant more access than is required).
- Need to Know: a principle that ensures access to information is limited to the specific information that a user needs to know to perform authorized job duties. Similar to Least Privilege, FileLocal shall grant access to staff for only the data and information that staff legitimately need to know.

5. Roles and Responsibilities

1. PROGRAM MANAGER

The Program Manager is responsible for:

- Performing organizational self-assessment periodically to ensure compliance with this policy and related standards.
- Reviewing any technology acquisitions to determine if any clauses/statements are required in the contract with respect to compliance with this policy and related standards.
- Leading the investigation of any reported access control breaches in FileLocal computational environment.

- Ensuring that all employees are trained in regard to the applied access controls to FileLocal information resources.

2. FILELOCAL AGENCY

FileLocal is responsible for:

- Protecting information resources (i.e. data, systems, applications, network), whose ownership has been assigned to them, against unauthorized access.
- Authorizing and/or revoking privileges for access to information resources, whose ownership has been assigned to them.
- Understanding and managing access rights they have approved. As such, FileLocal shall periodically review all granted access and verify that the access continues as appropriate.
- Developing and maintaining the formal procedure for documenting, granting, changing, and terminating access to information resources, whose ownership has been assigned to them.
- Promptly reporting information security incidents to the CISO, or designee.
- Ensuring that users of their resources are complying with this policy and the associated standard and procedures. Taking the necessary corrective action where non-compliances with this policy are discovered.
- Ensuring that participating cities and vendors have undergone required security awareness training.

3. VENDORS

Vendors are responsible for:

- Implementing security controls that are mandated by this policy and related standards, for the systems of which they are in charge.
- Assisting the Program Manager, or their designee's, organizational self-assessment initiatives to confirm that FileLocal computational environment's components adhere to and are implemented in accordance with this policy and related standards.
- Identifying access control incidents, and reporting them to FileLocal and the Program Manager, or their designee.
- Assisting the Program Manager, or designee, in investigations in regard to access control breaches.
- Monitoring access control activities.
- Creating, managing, and terminating user accounts, including updating accounts when required access privileges change.
- Providing periodic reports to FileLocal and the Program Manager, or their designee.

4. PARTICIPATING CITIES

Participating Cities are responsible for:

- Accessing only the information resources to which they have been granted permission.
- Protecting FileLocal and its client's assets as an on-going responsibility of the business process and their individual task assignments.
- Identifying access control breaches and reporting them to FileLocal's Program Manager and a City's CISO, or their designee.
- Assisting the FileLocal Program Manager, or their designee, in investigations in regard to access control breaches.
- Monitoring access control activities.
- Creating, managing, and terminating user accounts.
- Providing periodic reports to FileLocal and a City's CISO, or designee.
- Promptly reporting violations of this policy and related standards (e.g. unauthorized access) to FileLocal's Program Manager and a City's CISO, or their designee.
- Understanding and following the Access Control Policy and related Standards.

6. Compliance

The Access Control Policy uses and assimilates the following bodies of recognized knowledge: ISO 27002:2013:

- Section 6.1.1 – Information Security Roles and Responsibilities
- Section 7.2.1 – Management Responsibilities
- Section 6.1.2 – Segregation of Duties
- Section 9 – Access Control

7. Related Documents

- Access Control Standard
- Identification and Authentication Standard
- Logical Access Control Standard
- Password Management Standard
- User Account Provisioning Standard

Encryption Policy

1. Introduction

Due to security exposures and risk, classified data is protected through the use of encryption technologies. Encryption technologies use complex mathematical formulae and techniques to protect the confidentiality, integrity and non-repudiation of communications and data. The Washington Multi-City Business License and Tax Portal Agency (FileLocal) uses encryption to protect classified data stored or transmitted through its information systems.

2. Purpose

The purpose of the Encryption Policy is to provide guidance on the use of encryption to ensure the confidentiality and integrity of classified information.

3. Scope

The Encryption Policy applies to those who utilize information systems, business applications, networks and information owned by FileLocal:

- Agency staff
- Temporary supplemental staff
- Contractors
- Vendors
- Consultants
- Participating cities
- All business partners and parties

The Encryption Policy also applies to all information systems, data, business applications and networks, used or administered by FileLocal and to all computational environments operated by, or operated on behalf of FileLocal.

Deviation from this policy is acceptable only if an information security threat and risk assessment has been completed with a documented business impact analysis and the Information Owner(s) have signed a risk acceptance form. The Risk Acceptance Form shall be authenticated by the Program Manager.

4. Policy Statements

A. Classified information shall always be transmitted or stored in encrypted form.

B. Cryptographic algorithms and tools shall be determined in line with policy by the Vendors in line with contractual requirements.

C. Cryptographic keys shall be protected during their entire life-cycle (generation, distribution, archiving, updating, revocation and destruction).

D. The applied cryptographic controls shall take into consideration data retention requirements.

E. Jurisdictional laws governing the use of encryption technology shall be used as legislated.

Roles and Responsibilities

1. PROGRAM MANAGER

The Program Manager is responsible for:

- Approving cryptographic algorithms, minimum key lengths, and tools for use to protect the classified FileLocal information.
- Reviewing architectural initiative(s) to determine compliance with FileLocal Encryption Policy and Standard.
- Performing organizational self-assessment annually to ensure compliance with this policy and related standard.
- Leading the investigation of any reported security breach in FileLocal computing environment.

2. FILELOCAL AGENCY

FileLocal is responsible for:

- Ensuring compliance with the encryption controls protecting the information resources.
- Ensuring that cryptographic key management is maintained according to the standard by vendors and participating cities.

3. VENDORS

Vendors are responsible for:

- Assisting Information Owners with the implementation of and the managing of encryption controls.
- Managing cryptographic keys in accordance with the requirements of this policy and related standard.
- Assisting the Executive with Information Security responsibilities' organizational self-assessment initiatives to confirm systems and infrastructure components adhere to and are implemented in accordance with this policy and related standard.
- Identifying and reporting security incidents to the Program Manager.

4. PARTICIPATING CITIES

Participating Cities are responsible for:

- Assisting Information Owners with the implementation of and the managing of encryption controls.
- Managing cryptographic keys in accordance with the requirements of this policy and related standard or managing cryptographic keys in accordance with the requirements and related standards of a City's CISO, or designee.
- Safeguarding assigned (personal) cryptographic keys.

- Immediately reporting violations of this policy (e.g. where cryptographic keys may have been compromised) to the Agency and a City's CISO, or designee.
- Understanding and following the Encryption Policy and related standard.

5. Compliance

The Encryption Policy uses and assimilates the following bodies of recognized knowledge: ISO 27002:2013:

- Section 12.3.1 – Information Back-up
- Section 13.1 – Network Security Management
- Section 13.2.1 – Information Transfer Policies and Procedures
- Section 9.4.3 – Password Management System
- Section 10 – Cryptographic Controls
- Section 18.1.5 – Regulation of Cryptographic Controls
- Section 13.1 – Network Security Management
- Section 14.1.3 – Protecting Application Services Transactions

6. Related Documents

- Encryption Standard

Infrastructure and Critical Vendor Policy (POL-040)

1. Introduction

The following policies and subsequent standards are expressly authored as foundation documents to manage Washington Multi-City Business License and Tax Portal Agency (FileLocal) infrastructure. In the marketplace reality - intrusion and unwarranted access and attacks, FileLocal must make its infrastructure safe, to protect its assets, employees, intellectual property, and taxpayer privacy. Attacks can come from external and internal sources and can cause significant loss and exposure to risks to both the business and its operations. Security controls must be in place to prevent security breaches from any source. It is unacceptable to have poorly or inadequately configured systems which can facilitate an attack and pose a high risk on critical information resources. All information systems must be deployed with secure configurations and maintained continuously to the highest standards, which are expressed in the standards documents.

2. Purpose

The purpose of the Infrastructure Policy is to articulate boundaries, scope, content, and other forms of intellectual capital that comprise FileLocal's governing principles on the security of its infrastructure, including that of critical vendors, such as Avenu and Kubra. Such expression of artifacts is intended to ensure that FileLocal's infrastructure is deployed and configured to provide the highest level of security for infrastructure components.

A second purpose is to set forth those security artifacts sufficient to ensure that security of information systems is maintained in an acceptable, useful and appropriate lifecycle.

3. Scope

The Infrastructure Policy applies to those who utilize information systems, business applications, networks and information owned by FileLocal:

- Full-time employees
- Part-time employees
- Temporary supplemental staff
- Contractors
- Consultants
- Vendors, including, but not limited to, Avenu and Kubra

The Infrastructure Policy also applies to all information systems, data, business applications and networks, used or administered by FileLocal and to all computational environments operated by, or operated on behalf of FileLocal.

Deviation from this policy is acceptable only if an information security threat and risk assessment has been completed with a documented business impact analysis and the FileLocal Agency Staff(s) have signed a risk acceptance form. The Risk Acceptance Form shall be authenticated by the Program Manager.

4. Policy Statements

A. Vendors and FileLocal shall manage their infrastructure in a manner that ensures its proper use, prevents unauthorized access or use, maintains availability and protects the security of information resources.

B. External users / systems / networks shall be allowed to connect to Vendor or FileLocal's networks only if the connection is required for a legitimate business need.

C. The security controls used by Vendors shall be commensurate with the classification level of stored, processed, or transmitted information in accordance with FileLocal's 'Information Classification Policy' and 'Information and Media Handling Standard'.

D. A formal risk assessment shall be performed on the infrastructure and critical vendors at least once a year. The risk assessment shall identify / confirm key risks imposed on the infrastructure and determine the security controls required to mitigate those risks within acceptable limits.

E. All user, system, application and network activities shall be logged to the extent that provides sufficient audit trail of those activities.

F. All documents created, stored, transmitted or received on FileLocal's computers and networks and on any attached removable devices shall be subject to monitoring by authorized personnel.

G. All security events shall be continuously monitored.

H. All monitored and logged activity on computational resources shall be reviewed by authorized personnel.

I. Equipment shall be maintained in accordance with the supplier's recommended service intervals and specifications.

5. Roles and Responsibilities

A. PROGRAM MANAGER

The Program Manager is responsible for:

- Developing and implementing strategies to ensure users are aware of using security policies, procedures, and benefits.
- Performing organizational self-assessment periodically to ensure compliance with this policy and related artifacts.
- Periodically evaluating effectiveness of security policies and procedures.
- Reviewing any planned technology acquisition(s) to determine if any clauses / statements are required in the contract with respect to compliance with FileLocal's security policies and standards.
- Reviewing any architectural initiative(s), including selecting vendors, to determine compliance with FileLocal's security policies and standards.
- Leading any investigation of any reported security breaches in FileLocal's or Critical Vendors' systems business applications or networks.
- Authorizing inbound and outbound traffic through the firewall - as needed by the business.

B. FILELOCAL AGENCY STAFF

FileLocal Agency Staffs are responsible for:

- Ensuring FileLocal's computational resources are configured to adhere to the controls mandated by this policy and related standards, where ownership has been assigned to them.
- Establishing and maintaining an inventory of computational resources (e.g. servers, desktops, laptops, network devices).
- Authorizing access privileges to the computational resources, where such ownership has been assigned to them.
- Promptly reporting security incidents to the FileLocal Executive with Information Security Responsibilities.
- Monitoring the quality of any IT service provided by Third Parties to ensure compliance with the SLA.
- Ensuring compliant security logging is implemented on the computational resources.
- Ensuring team members are compliant with this policy and related artifacts.
- Proceeding with necessary corrective actions where policy non-compliance has occurred with team members.
- Ensuring changes to those owned computational resources are documented and implemented.

C. CRITICAL VENDORS (INCLUDING AVENU AND KUBRA)

Critical Vendors are responsible for:

- Assisting FileLocal Agency Staff to implement and maintain security controls mandated by this policy and related artifacts.
- Providing assistance to the FileLocal Executive with Information Security Responsibilities' organizational assessment initiatives to confirm systems and infrastructure components adhere to and are implemented in accordance with this policy and related standards and procedures.
- Assisting Information Users on the use of infrastructure resources and solving technical problems in accordance with FileLocal Infrastructure Policy and Standards.
- Keeping up-to-date documentation pertaining to the infrastructure architecture and infrastructure components.
- Monitoring user, network and system activities; maintain the audit logs and ensure its continuous integrity.
- Performing security scans of perimeter devices bi-annually, to detect – non-compliance (e.g. unauthorized modems).
- Reviewing the configuration of infrastructure components on a regular basis.
- Identifying any non-compliant computational activities, and report such to FileLocal Agency Staff and the FileLocal Executive with Information Security Responsibilities.

- Recording security incidents relating to the infrastructure, report them to the FileLocal Executive with Information Security Responsibilities.
- Providing assistance to the FileLocal Executive with Information Security Responsibilities for investigations of security breaches in regard to the infrastructure.
- Providing periodic reports to FileLocal Agency Staffs and the FileLocal Executive with Information Security Responsibilities.

D. INFORMATION USERS

Information Users are responsible for:

- Accessing only those information resources to which they have been granted permission.
- Accessing FileLocal's information resources and Internet only via approved access points.
- Protecting access credentials and safeguarding portable computers from loss / theft.
- Protecting sensitive / confidential information on devices assigned to them.
- Ensuring that the use of computational resources (e.g. their devices, network devices, servers, etc.) is in compliance with the requirements mandated by this policy and related standards.
- Immediately reporting violations of this policy and related standards to Help Desk.
- Working within and respecting the intention / purpose /objectives of this Policy and related artifacts.
- Not changing or altering system and application security configuration of their computers/devices.
- Protecting FileLocal's and FileLocal's client information as a regular part of the business process and their individual work assignments.

6. Compliance

The Infrastructure Policy uses and assimilates the following bodies of recognized knowledge: ISO 27002:2013:

- Section 8.1 - Responsibility for assets
- Section 11.1 - Secure areas
- Section 11.2 - Equipment
- Section 12.1 - Operational procedures and responsibilities
- Section 12.1.3 Capacity Management
- Section 12.3 – Backup
- Section 12.4 – Logging and Monitoring
- Section 13 – Communications Security
- Section 13.1 - Network security management

- Section 14.2.9 System Acceptance Testing
- Section 15.2 - Supplier Service Delivery Management

7. Related Documents

- Remote Access Standard
- Perimeter Security Standard
- Wireless Standard
- Security Event Monitoring Standard
- Audit Trail Standard
- Laptop, PDA and Mobile Devices Standard
- Network and Network Devices Standard
- Server, Desktop and Mainframe Standard
- Vulnerability Management Standard
- System Hardening Standards

Physical and Environmental Security Policy (POL-50)

1. Introduction

Information resources require not only logical but also physical security controls to protect the confidentiality, integrity and availability of information and ensure proper and timely operation. Computer systems and facilities shall be protected from theft, unauthorized disruption of operation and damage caused by environmental hazards such as fire, dust, water, and other contaminants or the unplanned loss of power.

2. Purpose

The purpose of the Physical and Environmental Policy is to outline the principles that govern the implementation of physical security controls that protects the Washington Multi-City Business License and Tax Portal Agency (FileLocal) information resources. As the FileLocal staff utilize the City of Seattle's infrastructure for day-to-day work, the FileLocal staff are under the City of Seattle's CISO, or designee, policies around Physical and Environment as well. This policy is to further refine the specifics for the agency as a separate Municipal Non-Profit Corporation.

3. Scope

The Physical and Environmental Policy applies to those who utilize information systems, business applications, networks and information owned by FileLocal:

- Agency staff
- Temporary supplemental staff
- Contractors
- Vendors
- Consultants
- Participating cities
- All business partners and parties

The Physical and Environmental Policy also applies to all information systems, data, business applications and networks, used or administered by FileLocal and to all computational environments operated by, or operated on behalf of FileLocal.

The policy also applies to all facilities and physical areas that host any kind of information resources.

Deviation from this policy is acceptable only if an information security threat and risk assessment has been completed with a documented business impact analysis and FileLocal has signed a risk acceptance form. The Risk Acceptance Form shall be authenticated by the Program Manager.

4. Policy Statements

A. The applied physical access controls shall be commensurate with the identified risk and its impact on business processes.

B. Access to business facilities and restricted areas shall be restricted to authorized personnel only.

C. FileLocal shall ensure strong physical controls around handling visitors that access FileLocal colocation facilities.

D. FileLocal shall adopt clear desk practices according to the “Physical and Environmental Policy”.

E. FileLocal shall ensure physical intrusion detection system and surveillance systems (for example, CCTV), as appropriate to safeguard restricted colocation areas.

F. FileLocal shall apply appropriate safeguards against disruptive events such as fire, flood, and other environmental hazards.

G. FileLocal shall apply automatic alarm systems as necessary to notify Facility Security about environmental hazards.

H. FileLocal shall protect computer media and other information processing systems against theft.

I. Temperature and humidity shall be controlled in data processing facilities.

J. Equipment, information, and software shall not be taken off-site without appropriate authorization under the “IT Asset Management Policy”.

5. Roles and Responsibilities

A. Program Manager

The Program Manager is responsible for:

- Performing organizational self-assessment periodically to ensure compliance with this policy and related standard.
- Ensuring that all employees are trained in regard to the applied physical controls to FileLocal information resources.

B. FileLocal

FileLocal is responsible for:

- Protecting information resources (i.e. data, systems, applications, network), whose ownership has been assigned to them, against physical and environmental threats as well as unauthorized physical access
- Authorizing access to security areas that host information resources whose ownership has been assigned to them.

C. Vendors

Vendors are responsible for:

- Implementing security controls that are mandated by this policy and related standards, for the systems of which they are in charge.
- Assisting Executive with Information Security responsibilities organizational self-assessment initiatives to confirm that FileLocal computational environment’s components adhere to and are implemented in accordance with this policy and related standard.

D. PARTICIPATING CITIES

Participating Cities are responsible for:

- Following the security protocols established by a City's CISO, or designee, and ensuring the overlying policy is met.

6. Compliance

The Physical and Environmental Security Policy uses and assimilates the following bodies of recognized knowledge: ISO 27002:2013:

- Section 11.1.1 – Physical security perimeter
- Section 11.1.2 – Physical entry controls
- Section 11.1.3 – Securing offices, rooms, and facilities
- Section 11.1.4 – Protecting against external and environmental threats
- Section 11.1.5 – Working in secure areas
- Section 11.2.1 – Equipment siting and protection
- Section 11.2.3 – Cabling security
- Section 11.2.5 – Removal of property
- Section 11.2.9 – Clear Desk and Clear Screen Policy

7. Related Documents

- N/A

Third Party Management and Outsourced Services Policy (POL-060)

1. Introduction

In many situations, outsourcing offers a company a cost effective alternative to in-house capabilities. Outsourcing, however, does not reduce the fundamental risks associated with information technology or the business lines that use it. On the contrary, engaging external parties introduces new risk factors as the company's mandate to protect its business critical information partly relies on the security controls applied by the service provider.

Similarly, Third Party access to a company's information resources imposes risk on the integrity, confidentiality and availability of information and the continuity of business operation.

2. Purpose

The purpose of the Third Party Management and Outsourced Services Policy is to ensure contiguous security of Washington Multi-City Business License and Tax Portal Agency's (FileLocal's) information resources with respect to its computational environment when dealing with third parties and contracted entities.

3. Scope

The Third-Party Management and Outsourced Services Policy applies to those who utilize information systems, business applications, networks and information owned by FileLocal:

- Agency Staff,
- Temporary supplemental staff,
- Contractors,
- Consultants,
- All business partners and third parties, including Critical Vendors, such as Avenu and Kubra.

The Third-Party Management and Outsourced Services Policy also applies to all information systems, data, business applications and networks, used or administered by FileLocal and to all computational environments operated by, or operated on behalf of FileLocal.

The document will use "Third Parties" as a collective term to denote:

- Third parties not under contractual terms to FileLocal but providing a service to FileLocal as mutually agreed.
- Approved Third Parties that are to provide FileLocal with a commercial service under a yet to be executed agreement.
- Subcontractors providing services to FileLocal as employee equivalents or staff augmentation, who are obligated under master agreements, individual agreements and/or other such contracts.
- Trading Partners, (may or may not be within a mutually executed contract).
- Suppliers of products, services (including network services) and information.

- Suppliers of remote systems support and maintenance.
- Customers, as they may wish to conduct a commercial transaction in advance of or not requiring a form of contract,
- Any other entity needing to connect with FileLocal computational environment to provide a service as mutually agreed.

Deviation from this policy is acceptable only if an information security threat and risk assessment has been completed with a documented business impact analysis and the Information Owner(s) have signed a risk acceptance form. The Risk Acceptance Form shall be authenticated by the Program Manager.

4. Policy Statements

1. IT services shall be obtained from service providers that are capable of providing effective security controls.
2. Third party access and outsourced services shall be supported by documented contracts and/or service level agreements. These agreements shall:
   - Define the security service level commitments by the IT service provider and each Third Party.
   - Identify responsibilities for all parties involved, including responsibilities with respect to legal matters.
   - Mandate each Third Party's compliance with FileLocal's Information Management Policies and Standards.
   - Promote compliance with corporate governance, legal and regulatory requirements.
   - Govern the cooperation on investigation efforts of security incidents.
3. FileLocal shall require approval to the use of a third party's computational resources in advance of remote or internal access to FileLocal's computational resources.
4. The Confidentiality, Integrity and Availability of data shall be protected over connections with Third Parties and on computational resources owned by Third Parties. The level of protection required shall be determined by assessing the risk to business requirements.
5. No Third Party connection shall be authorized without evidence that relevant Information Owner(s) have completed a formal assessment and acceptance of the risk to the shared infrastructure.
6. Third Parties shall access FileLocal's computational resources using hardware, software and network components as per agreement.
7. Third Party's artifacts including, but not limited to, risk assessment document, configuration details, etc. shall be maintained and access provided to authorized staff only.
8. Information Owners shall monitor the security of service provided by each Third Party and ensure compliance with the contracted SLA.
9. Any change in a Third Party's access shall follow FileLocal's Change Management Process. Security and privacy concerns of FileLocal shall be addressed in the change management process performed by the vendor

10. FileLocal shall have the right to audit the security measures at each Third Party and third party devices accessing FileLocal's computational resources, or be provided with the most recent external audit of Third Party's information system SSAE 18, SOC 2 related to the service being provided to ensure compliance with the agreement.
11. Each Third Party connection shall be reviewed regularly to confirm a continuing business need.
12. Each Third Party access shall be removed immediately, when the business relationship with that Third Party terminates / ceases or Third Party's access is no longer required.
13. Third Parties shall receive appropriate training and regular updates in FileLocal's information security policies and standards. This includes security requirements, legal responsibilities, and business controls, as well as training in the correct use of information processing facilities, before access to information or services is granted.
14. Third Party agents working in secure areas shall be supervised at all times to prevent opportunities for malicious activities.
15. Non-disclosure agreements should be signed where appropriate.

5. Roles and Responsibilities

5.1 Program Manager

The Program Manager is responsible for:

- Performing organizational self-assessment periodically to ensure compliance with this policy and related standards.
- Periodically evaluating the effectiveness of security policies and procedures.
- Reviewing any third party agreement(s) to determine compliance with FileLocal information security policies and standards.
- Leading the audit exercise against Third Party information resources.
- Leading the investigations in regard to Third Party access control breaches.

5.2 FileLocal

FileLocal is responsible for:

- Assessing risk arising from Third Party access.
- Authorizing Third Party access to information resources, whose ownership has been assigned them.
- Revoking authorization for Third Party access when the business/contractual relationship ends.
- Promptly reporting information security incidents to the Executive with Information Security responsibilities.
- Monitoring the security of service provided by each Third Party to ensure compliance with the SLA.

- Ensuring that Third Party users of their resources are complying with this policy and taking the necessary corrective action where deviation from this policy is discovered.
- Ensuring that security and privacy concerns are addressed at all parts of the project management process.

5.3 Critical Vendors (Including, but not limited to, e-Gov and Kubra)

Critical Vendors are responsible for:

- Ensuring that Third Parties working with FileLocal information resources follow this policy.
- Assisting the Executive with Information Security Responsibilities' organizational self-assessment initiatives to confirm that FileLocal computational environment's components adhere to and are implemented in accordance with this policy.
- Identifying access control breaches, and reporting them to Information Owners and the Executive with Information Security responsibilities.
- Assisting the Executive with Information Security responsibilities in investigations in regard to Third Party access control breaches.
- Monitoring access control activities.
- Creating, managing and terminating Third Party user accounts.
- Providing periodic reports to FileLocal and the Executive with Information Security responsibilities.
- Ensuring that security and privacy concerns are addressed at all parts of the project management process

6. Compliance

The Third-Party Management and Outsourced Services Policy uses and assimilates the following bodies of recognized knowledge: ISO 27002:2013:

- **Section** 6 – Organization of Information Security
- Section 7.2.2 - Information security awareness, education, and training
- Section 9.1 - Business Requirement for Access Control
- Section 9.2 - User Access Management
- Section 9.4 – System and application access control
- Section 11.1.2 - Physical entry controls
- Section 12.4.1 - Event logging
- Section 13.1.1 – Network Controls
- Section 13.2.4 - Confidentiality or non-disclosure agreements

Section 15.1.2 - Addressing security within supplier agreements

7. Related Documents

- N/A

Data Backup (POL-070)

1. Introduction

Each company faces multiple intentional and unintentional threats that could cause the loss, corruption, or temporary unavailability of data such as hardware failures, accidental deletion, incorrect modification, software corruption, and malicious activities. As these threats occur quite frequently, it is essential that backup copies of business critical information are maintained diligently. Backup copies ensure the continued availability and viability of the information when these threats occur.

2. Purpose

The purpose of the Data Backup Policy is to outline the principles that govern the implementation of backup and recovery controls, which ensure the availability of the Washington Multi-City Business License and Tax Portal Agency (FileLocal) information resources.

3. Scope

The Data Backup Policy applies to those who utilize information systems, business applications, networks and information owned by FileLocal:

- Agency staff
- Temporary supplemental staff
- Contractors
- Vendors
- Consultants
- Participating cities
- All business partners and parties

The Data Backup Policy also applies to all information systems, data, business applications and networks, used or administered by FileLocal and to all computational environments operated by, or operated on behalf of FileLocal.

Deviation from this policy is acceptable only if an information security threat and risk assessment has been completed with a documented business impact analysis and the FileLocal have signed a risk acceptance form. The Risk Acceptance Form shall be authenticated by the Executive with Information Security responsibilities.

4. Policy Statements

A. FileLocal business critical information shall be backed up so that it can be restored when required.

B. Data backup periods shall be defined based on business requirements. These requirements shall be determined based on the acceptable data loss in case of a disruption.

C. When the acceptable data loss is less than the period between the backup jobs, backups shall be coupled with other information retention methods (e.g. transaction logs, mirroring, clustering, and fail-over capabilities).

D. Backup retention shall be implemented in accordance with the "Information Retention Standard".

E. Backups have the same sensitivity level as the data stored on them, according to the Information Classification Policy.

F. FileLocal shall regularly test the backup and restore procedures and equipment.

G. Backup media shall be handled in accordance with the Data Storage Media Library Management Policy and all current vendor contracts

H. Off-site backup shall be maintained in a secure location, separate from FileLocal data center.

I. Security controls for media held at remote locations shall be the same as at the main sites.

J. FileLocal shall develop and implement detailed procedures for performing backups, restoring data, performing testing of backups, transferring tapes to/from the storage facility, and recycling or disposing of backups upon expiration of their retention period.

5. Roles and Responsibilities

A. FileLocal Executive with Information Security responsibilities Executive with Information Security responsibilities is responsible for:

- Performing organizational self-assessment periodically to ensure compliance with this policy and related artifacts.
- Leading investigations of any reported control breaches with regards to data backup and restoration.
- Ensuring that all FileLocal staff are trained with regards to the applied data backup controls.

B. FileLocal

FileLocal is responsible for:

- Ensuring that data, whose ownership has assigned to them, are backed up in accordance to this policy and related artifacts.
- Ensuring that formal procedures for data backup and restoration are developed.
- Promptly reporting information security incidents to the Executive with Information Security responsibilities.

C. Vendors

Vendors are responsible for:

- Implementing security controls that are mandated by this policy and related artifacts, for the systems of which they are in charge.
- Backing up and restoring any FileLocal information stored on their systems.

- Assisting Executive with Information Security responsibilities organizational self- assessment initiatives to confirm that FileLocal computational environment's components adhere to and are implemented in accordance with this policy and related artifacts.
- Responding to access control breaches and reporting them to FileLocal and the Executive with Information Security responsibilities.
- Assisting the Executive with Information Security responsibilities in investigations of breaches with regards to data backup and restoration.
- Developing and maintaining data backup procedures.

D. Participating Cities

Participating Cities are responsible for:

- Ensure that systems of record have appropriate storage and backup facilities. An annual attestation to this will be sent FileLocal annually.
- Understanding and following the Data Backup Policy and related artifacts and following a City's CISO, or designee, Information Security polices related to data backup.

6. Compliance

The Data Backup Policy uses and assimilates the following bodies of recognized knowledge: ISO 27002:2013:

- Section 7.1.2 – Ownership of assets
- Section 7.2.2 – Information labeling and handling
- Section 9.1.2 – Physical entry controls
- Section 10.5.1 – Information back-up
- Section 10.7 – Media Handling

7. Related Documents

- Information Retention Standard

Data Storage Media Library Management Policy(POL-080)

1. Introduction

Critical information is stored on backup tapes and other media as part of the Washington Multi-City Business License and Tax Portal Agency (FileLocal) operational procedures. The media must be protected from unauthorized disclosure, abuse and physical damage as information stored on these media is subjected to a variety of human and environmental threats.

2. Purpose

The purpose of the Data Storage Media Library Management Policy is to outline the principles that govern the implementation of media library management controls to protect the content of the storage media.

3. Scope

The Data Storage Media Library Management Policy applies to those who utilize information systems, business applications, networks and information owned by FileLocal:

- Agency staff
- Temporary supplemental staff
- Contractors
- Vendors
- Consultants
- Participating cities
- All business partners and parties, including critical vendors, such as e-Gov and Kubra.

The Policy also applies to all information systems, data, business applications and networks, used or administered by FileLocal and to all computational environments operated by, or operated on behalf of FileLocal.

The Data Storage Media Library Management Policy applies to all data storage media such as magnetic tapes, magnetic or optical cartridges, disks and diskettes, or solid state storage technologies.

Deviation from this policy is acceptable only if an information security threat and risk assessment has been completed with a documented business impact analysis and the FileLocal have signed a risk acceptance form. The Risk Acceptance Form shall be authenticated by the Program Manager.

4. Policy Statements

A. FileLocal shall be able to track the content, location, security classification (for example, copying restrictions) and identification of FileLocal data for all media.

B. All media shall be labelled with a unique identifier, ownership information, security classification, and any necessary handling requirements.

C. If no longer required, the previous contents of any reusable media to be removed from FileLocal shall be sanitized.

D. Authorization shall be required for any media to be removed from FileLocal premises. A record of all such removals shall be kept to ensure accountability.

E. All media shall be stored in a safe, secure environment, in accordance with manufacturers' specifications and regulatory requirements.

F. All information stored on media shall be protected according to the Information Classification Policy and related standard.

5. Roles and Responsibilities

A. Program Manager

The Program Manager is responsible for:

- Performing organizational self-assessment periodically to ensure compliance with this policy and related standards.
- Leading the investigation of any reported breaches in FileLocal computational environment in regard to media library management.
- Ensuring that appropriate personnel are trained in regard to the applied media library management controls.

B. FileLocal

FileLocal is responsible for:

- Performing organizational self-assessment periodically to ensure compliance with this policy and related standards.
- Leading the investigation of any reported breaches in FileLocal computational environment in regard to media library management.
- Ensuring that appropriate personnel are trained in regard to the applied media library management controls.

C. Vendors

Vendors are responsible for:

- Implementing security controls that are mandated by this policy and related artefacts, for the systems of which they are in charge.
- Assisting Executive with Information Security responsibilities organizational self-assessment initiatives to confirm that FileLocal computational environment's components adhere to and are implemented in accordance with this policy and related standards.
- Identifying control breaches in regard to media library management (e.g. missing media or any deviation to this policy), and reporting them to FileLocal and the Executive with Information Security responsibilities.

- Assisting the Executive with Information Security responsibilities in investigations in regard to media library management breaches.
- Understanding and following the requirements mandated by this policy and related artifacts.

D. PARTICIPATING CITIES

Participating Cities are responsible for:

- Assisting the Executive with Information Security responsibilities in investigations in regard to media library management breaches.
- Understanding and following the requirements mandated by this policy and related artifacts and following a City's CISO, or designee, information security policies related to this policy.

6. Compliance

The Data Storage Media Library Management Policy uses and assimilates the following bodies of recognized knowledge: ISO 27002:2013:

- Section 8.1.1 – Inventory of assets
- Section 8.1.2 – Ownership of assets
- Section 8.2.2 – Labeling of information
- Section 8.2.3 – Handling of assets
- Section 11.2.5 – Removal of assets
- Section 8.3.1 – Management of removable media
- Section 8.3.2 – Disposal of media
- Section 8.3.3 – Physical media transfer
- Section 12.4.1 – Audit logging
- Section 9.2 – User Access Management

7. Related Documents

- N/A

Compliance (POL-90)

1. Introduction

The management of information and the design, operation, use of and management of information systems are subject to statutory, regulatory and contractual security requirements. The Washington Multi-City Business License and Tax Portal Agency (FileLocal) is legally obligated to comply with such regulations and to ensure to its stakeholders that criteria are met or surpassed.

2. Purpose

The purpose of this policy is to ensure compliance with statutory and regulatory requirements and alignment with ISO Standard Information technology — Security techniques — Code of practice for information security management (ISO 27002:2013) and industry best practices such as Control Objectives for Information and related Technology (COBIT) version 4.

3. Scope

The Compliance Policy applies to those who utilize information systems, business applications, networks and information owned by FileLocal:

- Agency staff
- Temporary supplemental staff
- Contractors
- Vendors
- Consultants
- Participating cities
- All business partners and parties

The Compliance Policy also applies to all information systems, data, business applications and networks, used or administered by FileLocal and to all computational environments operated by, or operated on behalf of FileLocal.

Deviation from this policy is acceptable only if an information security threat and risk assessment has been completed with a documented business impact analysis and the FileLocal have signed a risk acceptance form. The Risk Acceptance Form shall be authenticated by the Executive with Information Security responsibilities.

4. Policy Statements

A. Statutory, regulatory and contractual requirements shall be defined and documented for use by information, computational resources and processes. Note that legislative requirements vary from country to country and may vary when information is intended for trans-border data flow, e.g. created in one country then transmitted to another country.

B. Changes in all relevant statutory, regulatory and contractual requirements shall be reviewed on a regular basis.

C. Changes in the information management policies shall be in accordance with FileLocal operating procedures.

D. Legal restrictions shall apply to the usage of material with any associated intellectual property rights, such as copyright, trademarks, patents.

E. FileLocal records shall be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

F. Data protection and privacy shall adhere to relevant legislation, regulations.

G. Cryptographic controls shall be applied to comply with relevant agreements, laws, and regulations.

H. Software license conditions shall be validated annually.

I. FileLocal staff, contractors, and service providers shall comply with FileLocal information security policies, standards, procedures and guidelines.

J. Users shall be educated on, monitored for, and reported on unauthorized use of FileLocal computational resources.

K. Agency staff awareness shall be reinforced annually on information security policies and standards and disciplinary actions for non-compliance.

L. External Third-Party expert resources shall perform annual reviews to ensure compliance to FileLocal information security policies and standards.

M. Information management policies and standards shall be reviewed annually and updated as necessary.

N. Information security procedures and guidelines shall be reviewed semi-annually and updated as necessary.

O. Compliance assessments shall be planned to minimize risk and disruptions to business processes.

5. Roles and Responsibilities

A. Chief Information Officer

Chief Information Officer (CIO) is responsible for:

- Ensuring compliance with software licensing.

B. Executive with Information Security responsibilities

Executive with Information Security responsibilities is responsible for:

- Performing organizational self-assessment periodically to ensure compliance with this policy and related standards.
- Leading the investigation of any reported non-compliance issues.
- Ensuring that all employees are trained in regard to the applied controls and disciplinary actions for non-compliance.

- Defining relevant statutory, regulatory and contractual obligations into compliance requirements.
- Identifying relevant changes from authorized sources that affect FileLocal information security policies, and standards.
- Reviewing policies, standards annually.

C. FileLocal

FileLocal is responsible for:

- Ensuring information and computational resources within their areas of responsibility are handled and managed to achieve compliance with FileLocal information security policies and standards.
- Reporting suspected security compromises for non-compliance to the Executive with Information Security responsibilities.

D. Vendors

Vendors are responsible for:

- Implementing security controls that are mandated by this policy and related standards, for the systems of which they are in charge.
- Assisting Executive with Information Security responsibilities organizational self- assessment initiatives to confirm that FileLocal computational environment's components adhere to and are implemented in accordance with this policy and related standards.
- Immediately reporting security compromises / non-compliance to the Executive with Information Security responsibilities.
- Assisting the Executive with Information Security responsibilities in investigations in regard to access control breaches.

E. Participating Cities

Participating Cities are responsible for:

- Respecting intellectual capital / property rights.
- Using software legally.
- Promptly reporting violations of FileLocal information security policies and standards to Help Desk.
- Adhering to FileLocal information security policies and standards.

F. Internal Audit

Internal Audit is responsible for:

- Ensuring adherence to information security policies and standards through periodic compliance assessments.

-

6. Compliance

The Compliance Policy uses and assimilates the following bodies of recognized knowledge: ISO 27002:2013:

- Section 6.1.8 – Independent Review of Information Security
- Section 7.1.3 – Acceptable use of Assets
- Section 10.1.2 – Change Management
- Section 15.1 – Compliance with Legal Requirements
- Section 15.1.2 – Intellectual Property Rights
- Section 15.1.3 – Protection of organizational records
- Section 15.1.4 – Data Protection and Privacy of Personal Information
- Section 15.1.5 – Prevention of Misuse of Information Processing Facilities
- Section 15.1.6 – Regulation of Cryptographic Controls
- Section 15.2.1 – Compliance with Security Policies and Standards
- Section 15.2.2 – Technical Compliance Checking
- Section 15.3.1 – Information Systems Audit Controls

7. Related Documents

- Acceptable Use Standard
- Security Assessment and Audit Standard

Incident Response Policy (POL-100)

1. Introduction

Businesses are subject to intrusions by unauthorized parties more than ever for a variety of reasons. Responding to security incidents and security events is an important component of the Washington Multi-City Business License and Tax Portal Agency (FileLocal) information security operations.

A strategy for managing security incidents requires the use of technologies and business practices aimed at prevention and mitigation. Preventive activities are based on measuring risk and applying various means to lower the number of security incidents and minimize anticipated resultant damage. Regrettably, not all security incidents can be prevented. To mitigate and manage a security incident requires a security incident response and reaction capability that is necessary to rapidly detect incidents, minimize loss and destruction, restore the assets as soon as possible, and improve practices based on the weaknesses exploited.

2. Purpose

The purpose of the security Incident Response Policy is to provide direction as to FileLocal preferred approaches to managing security incidents to protect assets and resources. FileLocal security Incident Response Policy is intended to frame processes and resources (trained staff) to manage security related problems and incidents to minimize business impacts professionally, including:

- Responding to incidents systematically.
- Helping personnel to recover quickly and efficiently from security incidents.
- Using information and knowledge gained during security incident to better manage and prepare for potential future security incidents.

3. Scope

The Incident Response Policy applies to those who utilize information systems, business applications, networks and information owned by FileLocal:

- Agency staff
- Temporary supplemental staff
- Contractors
- Vendors
- Consultants
- Participating cities
- All business partners and parties

The Incident Response Policy also applies to all information systems, data, business applications and networks, used or administered by FileLocal and to all computational environments operated by, or operated on behalf of FileLocal.

A 'Security Incident' is an adverse event that compromises the security of a system, a network, information, physical assets, and/or the safety of employees. A 'Security Incident' includes malicious activities such as viruses, hacker attacks, stealing hardware or software or other assets, and unauthorized access to classified information. Security Incidents are categorized as follows:

- Physical (Threat or intrusion)
- Logical (attempts or actual unauthorized intrusions)
- Compliance based
- Awareness based

Deviation from this policy is acceptable only if an information security threat and risk assessment has been completed with a documented business impact analysis and the FileLocal have signed a risk acceptance form. The Risk Acceptance Form shall be authenticated by the Program Manager

4. Policy Statements

A. All Security Incidents shall be responded to as they occur or become known to FileLocal.

B. Incidents shall be categorized and prioritized based on the impact of the problem on the business.

C. Security Incidents shall be reported immediately in the following manner:

   I Users and Contracted Service Providers shall report a security incident to the Help Desk. II FileLocal and Custodians shall report security incidents to the Program Manager.

D. FileLocal supports a 'Whistle Blower' arrangement where the Program Manager shall receive a suspected security incident notification in secret.

E. FileLocal staff shall receive regular training relating to the action steps to be performed in the event of a security incident.

F. Incident response activities shall be escalated if necessary so that further damage can be avoided.

G. FileLocal staff, participating cities and suppliers shall have a plan for escalation and notification, based on the impact of the problem on the business.

H. Contact information and points of contact with law enforcement authorities, regulatory bodies, information service providers and media shall be maintained.

I. Vendors shall investigate and identify the causes of incidents, based on the impact and risk for the business.

J. Chain of custody shall be followed to be able to present the evidence in court.

K. Vendors shall form a Computer Security Incident Response Team.

L. Vendors shall apply appropriate diagnostic tools for effectively diagnosing the causes of an incident.

M. Third party contracts shall support cooperation on investigation efforts on security incidents.

N. Security incident response process shall be monitored to ensure compliance.

O. Roles and Responsibilities

A. PROGRAM MANAGER

The Program Manager is responsible for:

- Working with law enforcement authorities.
- Engaging Corporate Communications to ensure only appropriate information is released.
- Maintaining contacts with law enforcement authorities, regulatory bodies, information service providers and media.

B. FILELOCAL

FileLocal is responsible for:

- Promptly reporting information security incidents to the Executive with Information Security responsibilities.
- Ensuring security incident response procedures are in place and useful for their resources.
- Providing ongoing support and resources to Computer Security Incident Response Team (CSIRT).

C. VENDORS

Vendors are responsible for:

- Implementing security controls that are mandated by this policy and related standard, for the systems of which they are in charge.
- Assisting Executive with Information Security responsibilities organizational self- assessment initiatives to confirm that FileLocal computational environment's components adhere to, and are implemented in accordance with this policy and related standard.
- Contributing constructively to security incident response procedures to make them efficient and useful.
- Documenting activities and observations used in the security incident response process, to contribute to incident response best practice improvements.
- Determining incidents that meet 'false positive' criteria.
- Communicating security incident alerts to the Executive with Information Security responsibilities.
- Providing technical expertise, as a resource, to CSIRT.
- Performing organizational self-assessment periodically to ensure compliance with this policy and related standard.
- Assessing, categorizing and analyzing security incidents.
- Leading security investigations.
- Directing the Computer Security Incident Response Team.
- Escalating security incidents as necessary.

- Providing recommendations to resolve security incidents.
- Ensuring the cause of security incidents has been identified and addressed.
- Ensuring security incidents are resolved.
- Communicating / disseminating security incident information / reports to Executive Management, affected users and clients as required.
- Ensuring security incident response activities are documented.
- Ensuring staff receive training to ensure incident response procedures are understood.
- Ensuring that related processes (e.g. Incident Response, Escalation and Notification processes) are in place and useful and can be invoked as an intermittent unscheduled business process.
- Ensuring a repository of occurred security incidents is maintained.
- Ensuring the chain of custody is followed.

5. Participating Cities

Participating Cities are responsible for:

- Promptly reporting security incidents to Help Desk and to a City's CISO, or designee, in accordance to the Information Security Policies adopted.
- Co-operating with and contributing to the security incident response activities as required.

6. Compliance

The Incident Response Policy uses and assimilates the following bodies of recognized knowledge: ISO 27002:2013:

- Section 6.1.3 – Contact with Authorities
- Section 15.1.2 – Addressing security within supplier agreements
- Section 8.2.1 – Classification of information
- Section 16.1.1 – Responsibilities and procedures
- Section 16.1.2 – Reporting information security events
- Section 16.1.6 – Learning from information security incidents
- Section 16.1.7 – Collection of evidence

7. Related Documents

- Incident Response Procedure

Security Risk Assessment (POL-110)

1. Introduction

Information Security Risk Assessments (RA) are a necessary component to understanding the overall susceptibility of the organization to negative outcomes during normal operations. Assessment of risk utilizing a well understood methodology will produce results which can be compared on a time line basis.

2. Purpose

To require the Washington Multi-City Business License and Tax Portal Agency (FileLocal) to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

3. Scope

The Security Risk Assessment Policy applies to those who utilize information systems, business applications, networks and information owned by FileLocal:

- Agency staff
- Temporary supplemental staff
- Contractors
- Vendors
- Consultants
- Participating cities
- All business partners and parties

The Security Risk Assessment Policy also applies to all information systems, data, business applications and networks, used or administered by FileLocal and to all computational environments operated by, or operated on behalf of FileLocal.

Deviation from this policy is acceptable only if an information security threat and risk assessment has been completed with a documented business impact analysis and the FileLocal have signed a risk acceptance form. The Risk Acceptance Form shall be authenticated by the Chief Information Security Officer (CISO), or designee.

4. Policy Statements

A. All RA activities shall be conducted under a single planning authority to ensure that full coverage of the environment is maintained.

B. RAs shall be conducted on any information system, including applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained

C. RAs shall be conducted not more than annually.

D. RAs shall be conducted on any entity which has signed a third party agreement with FileLocal.

E. The execution, development and implementation of remediation programs is the joint responsibility of Information Security and the department responsible for the system area being assessed.

5. Roles and Responsibilities

A. Executive with Information Security responsibilities

Executive with Information Security responsibilities is responsible for:

- Leading all RA projects.
- Ensuring that the summary of all RAs is maintained.
- Approving the recommended remediation activities.

B. FileLocal

FileLocal are responsible for:

- Ensuring completeness of information supplied to staff performing RA activities.

C. Vendors

Vendors are responsible for:

- Assisting the RA staff in performing the activity.
- Implementing recommended remediation activities.
- Notifying the Executive with Information Security responsibilities in the case of a situation which would cause a change in assessment.

D. Participating Cities

Participating Cities are responsible for:

- A City's CISO, or designee, will participate in any ongoing RA activities.

6. Compliance

The Security Risk Assessment Policy uses and assimilates the following bodies of recognized knowledge:

ISO 27002:2013:

- Section 4 – Risk Assessment and Treatment

7. Related Documents

- PRO-310 Risk Management Process

System Development Life Cycle (SDLC) Policy

1. Introduction

The Washington Multi-City Business License and Tax Portal agency (FileLocal) is committed to a formalized System Development Life Cycle (SDLC) in support of its numerous publicly available software products in addition to its core data management business.

Ensuring that the SDLC includes information management and information security is a key differentiator.

2. Purpose

The purpose of System Development Life Cycle Policy is to set a minimum set of requirements which all system development projects must adhere to prior to being permitted into production use.

3. Scope

The System Development Life Cycle Policy applies to those who utilize information systems, business applications, networks and information owned by FileLocal:

- Agency staff
- Temporary supplemental staff
- Contractors
- Vendors
- Consultants
- Participating cities
- All business partners and parties

The System Development Life Cycle Policy also applies to all information systems, data, business applications and networks, used or administered by FileLocal and to all computational environments operated by, or operated on behalf of FileLocal.

Deviation from this policy is acceptable only if an information security threat and risk assessment has been completed with a documented business impact analysis and the FileLocal have signed a risk acceptance form. The Risk Acceptance Form shall be authenticated by the Program Manager.

4. Policy Statements

A. All new system development or major changes to existing systems shall consider data confidentiality, availability and integrity in its life cycle stages.

B. Systems to be developed shall be categorized, in accordance with the FileLocal Information Classification Policy, based on the level of the highest classification data component processed, inputted, outputted, stored or transmitted.

C. Risk assessments shall be performed to identify security risks of all systems to be developed, acquired or enhanced.

D. Security requirements of systems shall be identified during the specifications and design phases, prior to development and implementation.

E. All systems shall be tested thoroughly before being deployed into the production environment.

F. All production data shall be sanitized before being used as test data.

G. The software development life cycle shall adopt industry best practices and security recommendations.

H. Authentication methods shall be implemented in systems and system components to be developed or enhanced to prevent unauthorized access.

I. All user input shall be validated to prevent exploitation of input vulnerabilities.

J. Output data shall be validated to ensure that processing of data is correct.

K. Cryptographic controls shall be applied to protect data integrity and confidentiality according to the Information Classification and Encryption policies and related artifacts.

L. Major enhancement of existing systems shall be in accordance with FileLocal Documentation governance process.

M. The security specifications for system development and enhancements shall be reviewed and approved by the Executive with Information Security responsibilities.

N. All external and internal interfaces of systems to be developed or enhanced shall be documented.

O. Systems must be certified and accredited before being moved into production environment.

5. Roles and Responsibilities

A. Program Manager

The Program Manager is responsible for:

- Defining criteria used in the supporting standards.
- Reviewing design decisions.
- Providing consulting on appropriate methods.

B. FileLocal

FileLocal is responsible for:

- Ensuring projects are compliant with this policy.

C. Vendors

Vendors are responsible for:

- Implementing requirements for operations based on the SDLC design criteria. Assisting the FileLocal in understanding the implications of SDLC decisions.

D. PARTICIPATING CITIES

Participating Cities are responsible for:

- Adhering to this policy and associated standards as well as adopted Information Security polices at a City.

6. Compliance

The System Development Life Cycle Policy uses and assimilates the following bodies of recognized knowledge: ISO 27002:2013:

- Section 14.1.2 - Securing application services on public networks
- Section 12.5 – Control of operational software
- Section 14.2 – Security in Development and Support Processes

7. Related Documents

- Secure Application Development Standard

Business Continuity Policy (POL-140)

1. Introduction

Business Continuity addresses the preservation of business. In the event of disruptions caused by natural or deliberate events, it is essential that the Washington Multi-City Business License and Tax Portal Agency (FileLocal) sustain critical processes and operations in the face of business- threatening emergencies.

2. Purpose

This policy document outlines the security principles, requirements, and accountabilities for developing a Business Continuity Process for FileLocal

3. Scope

The Business Continuity Policy applies to those who utilize information systems, business applications, networks and information owned by FileLocal:

- Agency staff
- Temporary supplemental staff
- Contractors
- Vendors
- Consultants
- Participating cities
- All business partners and parties

The Business Continuity Policy also applies to all information systems, data, business applications and networks, used or administered by FileLocal and to all computational environments operated by, or operated on behalf of FileLocal.

Deviation from this policy is acceptable only if an information security threat and risk assessment has been completed with a documented business impact analysis and the FileLocal have signed a risk acceptance form. The Risk Acceptance Form shall be authenticated by the Program Manager.

4. Policy Statements

A. FileLocal shall implement a Business Continuity process to protect critical business operations and reduce disruptions to an acceptable level.

B. The Business Continuity Process shall include a combination of preventative and recovery measures.

C. Each of FileLocal business functions shall develop the necessary processes and infrastructure relevant to their aspect of the business to support the overall Business Continuity objectives.

D. The Business Continuity Plan (BCP) and supporting Activation Procedures shall include:

- Conditions for activating the BCP.

- Documenting roles, responsibilities and emergency procedures.
- Prioritizing the critical processes.
- Documenting emergency procedures to allow recovery and restoration of all critical systems
- within required times.
- Assessment of external and internal business dependencies.
- Appropriate education and training of personnel in the emergency procedures.
- Documenting required resources and equipment for the Backup Operations Center (BOC).
- Documenting procedures for recovery of operations at the BOC.
- Documenting a testing and maintenance plan to assure the reliability of backup procedures
- and systems.
- Procedures for returning to normal business operations.

5. Roles and Responsibilities

A. Program Manager

The Program Manager is responsible for:

- Identifying and determining the conditions for plan activation.
- Identifying roles and responsibilities of individuals and their alternates responsible for execution of each component of the plan.
- Developing effective communication arrangements and processes for liaison with internal and external authorities including police, fire services, government agencies and media.
- Developing a regular testing and maintenance schedule for the contingency framework.
- Conducting awareness and education activities in support of the business continuity framework.

B. FileLocal

FileLocal is responsible for:

- Developing emergency procedures.
- Developing fail-over procedures that describe actions to be taken to move critical business processes to the backup operations center and to restore business operations within the required time periods.

C. Vendors

Vendors are responsible for:

- Assisting FileLocal with developing emergency procedures.
- Assisting FileLocal with developing fail-over procedures.

- Developing procedures for restoration to normal operations.
- Identifying and reporting Business Continuity events to the Executive with Information Security responsibilities.

D. PARTICIPATING CITIES

Participating Cities are responsible for:

- Understanding and following the Business Continuity Policy and any further information security policies at a City.

6. Compliance

The Business Continuity Policy uses and assimilates the following bodies of recognized knowledge: ISO 27002:2013:

- Section 17 – Information Security Aspects Of Business Continuity Management

7. Related Documents

- Business Continuity Plan

Guidelines for Information Owners and Custodians (GDE-200)

1. Introduction

These guidelines will assist the Washington Multi-City Business License and Tax Portal Agency (FileLocal) staff accountable for information assets and/or responsible for IT network operations, program development, database administration, and application system operations to understand and implement the FileLocal security standards. It is written in plain language for general dissemination and highlights the important aspects of the Security Standards.

2. Vendor Responsibilities

Kubra provides development services, and has ownership over the development process for, the mobile application provided by FileLocal, and Avenu provides tax filing services for FileLocal.

3. Owners – Asset Classification

In addition to the more traditional list of assets such as facility, land, equipment, money, and people, the list of agency assets also includes information used to support the agency. The agency's physical assets are protected because lost or damaged assets damage the agency's chances of success. In the same manner, protecting the agency's information assets enhances its chance of success.

Prudent asset security yields improved value for stakeholders and improved customer service.

Information Owners are those individuals who have the final agency responsibility for information, and information system, protection. They include Data, System, Application and Network Owners and can also be the Program Manager.

Responsibilities include:

- Classification of information and information systems.
- Authorization of access rights to their data / systems / application / network.

Owners define the criticality level for assets according to the following:

- Mission critical assets (high criticality level)
- Agency critical assets (medium criticality level)
- Non-critical assets (low criticality level)

DO

- Clearly identify all assets
- Maintain an up to date asset inventory

A. Asset inventory records should have information such as:

   a. Owner

   b. Type

   c. Criticality

d. Version if applicable

e. Location

B. Information Classification Scheme

There is a four-level classification scheme at FileLocal

- RESTRICTED: Compromise might result in a critical loss
- CONFIDENTIAL: Compromise might result in important or significant loss
- INTERNAL: Information that may be shared within FileLocal to users on a need-to- know basis
- PUBLIC: Information that can be shared with the public

DO

- Clearly identify the security classification of information you own, or originate, commensurate with the value of that data to FileLocal
- Maintain the classification of information you originate or own throughout its lifecycle
- Manage and communicate the creation, labelling, storage, transmittal and disposal of your information according to FileLocal requirements

A. DATA RETENTION

FileLocal is legally obligated to retain all operating records for various periods of time. Retention periods vary for different types of records and are mostly determined by statutory and regulatory requirements.

DO

- Keep all documents and data in accordance with City Of Seattle document retention guidelines.

Where the City Of Seattle guidelines do not specify a specific retention period,

- Keep terminated User information (e.g. files, e-mails) for 30 days.
- Keep Audit Trails on-line for 6 months and on secondary storage for an additional 30 months.

B. STORAGE MEDIA DISPOSAL

Data Storage Media Disposal is the process of eliminating information assets from media that is no longer required. Deleting 'RESTRICTED' and 'CONFIDENTIAL' information stored on media is not sufficient because only the file name has been removed from the directory table of contents. The information is still there until it is overwritten by new data.

The media should be rendered unreadable by a 'Secure Wiping Technique' or by the physical destruction of the media.

4. Owners – System Development

Security and functionality should be designed and developed at the same time. Developing and following a formalized Software Development Lifecycle (SDLC) process will achieve this goal. A formalized SDLC process consists the following major phases:

- Requirements definition
- Design
- Development
- Implementation
- Post-Implementation

A. Security in the Design

- Logical and physical separation of the development and production environments to ensure access to the production environment is not inadvertently granted to those with access to the development environment
- Network segregation to achieve separation of development sandbox-type systems and production systems
- Segregation of duties to achieve separation of development duties from system operational duties

DO

- Adhere to the Secure Software Design Principles
- Consider the following technical security controls be incorporated in systems:
    - Input data validation
    - Processing controls to detect errors in the processing
    - Access control
    - Logging feature
    - Cryptographic controls
- Put extra emphasis on testing systems being developed
- Adhere to the Change Control Process for adopting changes to the design

B. SECURE SOFTWARE DESIGN PRINCIPLES

When designing software systems, the following program design principles should be considered:

- **Least Privilege:** Only give users enough authorization to data to perform the required job
- **Fail Safe Defaults:** Default values for variables should enable safest, least privileged operational mode
- **Least Common Mechanism:** Anything which is shared among different programs can be a path for communication and a potential security hole, so as little data as possible should be shared
- **Economy of Mechanism:** Designs which are smaller and simpler are easier to inspect and trust
- **Complete Mediation:** Every access to every object should be checked
- **Open Design:** The application of open source methods to the creation of physical products, machines and systems
- **Separation of Privilege:** A system should ensure that multiple conditions are met before granting permissions to an object
- **Psychological Acceptability:** The system should not place an undue burden on its users

5. Custodians – Logical Access Control

A. AUTHENTICATION

Logical access controls protects systems from unauthorized access by the following means:

- **Identification:** Identifying users (e.g. based on username, account number)
- **Authentication:** Verifying users identity (e.g. password, cryptographic key)
- **Authorization:** Granting access to a subject to access a system

Authentication is the security mechanism that ensures the reliable identification of the individual. Strong authentication combines of any two of the following factors

- **Type 1:** Something the user knows (i.e. password)
- **Type 2:** A physical artifact the user requires (i.e. security token)
- **Type 3:** Something unique to each user's physiology (i.e. fingerprint, voiceprint)

B. Identification

Identification of individuals is based on User IDs

DO

- Assign unique User IDs.
- Follow the naming convention for User IDs.
- Create User IDs that are at least 6 characters in length.
- Make sure that the User ID assigned to a user follows that employee throughout their employment period at FileLocal and that User IDs are not re-used.

C. Passwords

Passwords should be easy to remember but difficult to guess. Temporary passwords are permitted when:

- A new User ID is being assigned.
- A user has forgotten a password.
- A user is locked out of her/his User ID.

DO

- Configure systems to enforce strong passwords.
- Configure systems for passwords to expire after 60 days.
- Change vendor-supplied default passwords.
- Ensure passwords are not displayed on the screen or stored in clear text.
- Ensure passwords are not revealed, apart from a temporary one.
- Lock user accounts after 3 unsuccessful login attempts.

D. Authorization

Assigning access rights should be based on the following three principles:

- **Segregation of Duties:** Having more than one person required to complete a task
- **Least Privileges:** Assigning the minimum required authorization for an individual to complete a task
- **Need to Know:** Limiting access to information based on individual's role Access right are granted by Information Owners (e.g. VPs, business unit leaders)

E. REMOTE ACCESS

Allowing access from outside into the FileLocal environment exposes the following risks:

- Unauthorized access
- Interception of data during transmission

DO

- Use strong encryption and (2-factor) authentication on all remote connections
- Log all remote login access attempts
- Set a 30-minute idle timeout on the remote access server
- Document all external connections
- Display a login banner containing a warning message

6. Custodians – User Provisioning

A. User Account Creation

IS Service Desk is responsible for creating, managing and terminating user accounts.

DO

- Assign a unique ID for each user
- Ensure new User IDs are not created by cloning an existing one
- Grant an initial temporary password to the new User ID and do not leave the password blank
- Obtain a signed access rights document from the user

B. User Account Management

User accounts are changed based on Human Resource's notices about user termination or changing roles. User IDs must be verified before resetting the password.

DO

- Obtain a user update or termination notification from Human Resources before changing / deleting a user account
- Review and change access rights if a user changes roles
- Disable user accounts immediately upon user termination or departure
- Ensure Information Owners review and approve all accesses to their assets
- Positively verify a user's identity prior to resetting a password

-

C. Third Party Account Management

User accounts are changed based on Human Resource's notices about user termination or changing roles. User IDs must be verified before resetting the password.

DO

- Verify the required contractual arrangements have been completed prior to user account creation
- Grant only sufficient access to third parties required to perform their job
- Ensure Information Owners review and approve all third party accesses to their assets
- Disable 3rd party access on the final date of the contract

7. Custodians – Infrastructure Security

A. Audit Trails

Audit trails provide accountability for the usage of FileLocal systems. Protecting the integrity of audit logs is crucial.

Audit Trails include the following information:

- Type of event
- Date and time of event
- User identification
- Origin or destination IP address of the attempt
- Identity or name of the affected data or system component or resource
- Success or failure of the activity

DO

- Enable automated log capability of systems
- Time-stamp audit trails by an accurate real time clock
- Synchronize system clocks
- Ensure classified data are not stored in the logs in clear text
- Protect the integrity and confidentiality of audit trails

B. Encryption

DO

- Use only approved encryption and hash algorithms (DES, SHA-1 and MD5 are NOT approved algorithms)
- Use only approved encryption key lengths (minimum 128 bit for AES, 112 bit for 3DES and 1024 for RSA)
- Transmit and store classified information (RESTRICTED and CONFIDENTIAL) in encrypted form

- Protect cryptographic keys during the life-cycle of the key from modification, destruction and unauthorized disclosure
- Change symmetric cryptographic keys on a 6-month basis

C. Infrastructure Security in Networks / Servers / Desktops

Networks consist of devices such as firewalls, IDS/IPS, routers, switches, VPN concentrators.

DO

- Backup device configuration files regularly
- Apply security patches and updates regularly
- Use encrypted connections for remote administration
- Disable clear text protocols
- Ensure changes follow the Change Management Process
- Change vendor default settings immediately
- Ensure devices provide logs on security events / access attempts
- Document device configurations
- Harden all systems to a baseline standard prior to deployment in the FileLocal infrastructure
- Ensure network incidents are recorded, review and resolved
- Disable web services running on the routers/switches
- Present users with warning banners at login
- Delete data securely when systems are decommissioned or retired

D. Infrastructure Security in Wireless LAN

Wireless communication technologies, also referred to as WLAN, consist of the following technologies:

- • WiFi 802.11x
- Infrared
- Bluetooth
- RF Wireless keyboard

Due to the lack of inherent security features, only WiFi 802.11x is permitted to be used on FileLocal premises.

DO

- Use WiFi Protected Access (WPA) instead of Wireless Equivalency Protocol (WEP)
- Disable SSID broadcast
- Use 128-bit encryption
- Use 802.1X port authentication
- Apply a strong authentication method, such as two-factor authentication
- Perform secure device authentication
- All vendor default settings are changed
- Disable access to reported stolen WLAN devices immediately
- Apply security patches for WLAN devices regularly
- Use encrypted connections for remote administration
- Enable logging on WLAN access points
- Perform a site survey prior to deploying a WLAN

DO NOT

- Allow ad hoc connections between stations

8. Custodians – Application, System and Network Operational Security

A. Patch Management

Patch management is performed according to the formal patch management process.

DO

- Obtain security patches from reputable sources
- Apply patches according to the Change Management Process
- Test security patches before deploying
- Ensure a rollback strategy is in place before applying patches
- Backup systems prior to the installation of new patches
- Apply automatic software updates and deployment when applicable
- Document installed patches including at minimum:
    - Name of the device
    - Name of the patch
    - Version of the patch
    - Date of installation
    - Name of the person who installed the patch
    - Any problems encountered

B. DATA BACKUP

DO

- Retain backup data according to Data Retention requirements
- Handle backups with the same care as the data stored on them
- Test backups, restore procedures and equipment regularly
- Transport backups in a secure manner and maintain off-site backups in a secure location

E. Malicious Attacks

There are several types of malicious threats to FileLocal personnel, data and systems. Past viral attacks were designed to damage or disrupt a system. Today's malicious code is designed to silently steal data for profit without doing noticeable damage that would alert the user to its presence.

DO

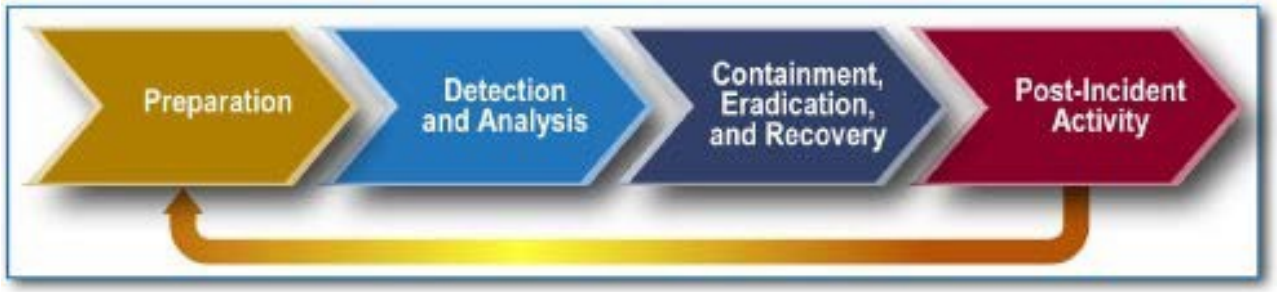
- Centrally manage and monitor antivirus products
- Ensure Antivirus software cannot be disabled on end user computers
- Apply antivirus software at email gateway
- Ensure antivirus software generates audit logs
- Update virus definitions automatically and regularly

9. Custodians – Physical Security

DO

- Obtain security clearance requests from Owners prior to granting access to FileLocal facilities.
- Maintain physical access logs for 3 months
- Physically secure publicly accessible network access points
- Close blinds in restricted area

10. Custodians – Responding to Security Incidents



When detected, there must be a structured response to security incidents so that the incident is dealt with quickly and comprehensively and forensic evidence can be collected if necessary. There are six stages to a structured security incident response:

Figure 1- Security Incident Response Process

- Preparation: This phase will be critical to ensuring that all other phases are performed adequately
- Detection and Analysis: This is the ability to identify incidents
- Containment: This isolates the systems affected by the incident
- Eradication: This removes the cause of the incident, for example deleting a virus
- Recovery: This restores and returns the system to operational status
- Post-Incident Activity: This is the investigation into the initial cause of the incident

DO

- Establish a Computer Security Incident Response Team (CSIRT) that responds to incidents
- Develop a structured incident response process
- Ensure FileLocal management is involved when rising incident severity warrants escalation
- Train and exercise CSIRT members in the incident response process
- Integrate Intrusion Detection System (IDS) and Security Incident and Event Management (SIEM) system with incident response process and IT operations
- Educate Service Desk personnel in incident detection techniques and incident escalation
- Collect and record information as an incident investigation evolves, including:
    - Current status of the incident
    - Actions taken during the Security Incident response
    - Actions taken by Security Investigators for each incident
    - A list of the evidence gathered during the incident investigation / analysis phase
    - Comments and notes ‘to-file’ or in any form from Security Investigators
    - Planned Steps to be started in a Security Investigation

11. Asset Inventory

11.1 Introduction

This inventory is intended as a reference for FileLocal to use to track all FileLocal information assets (servers, laptops, etc.) and should be updated on at least an annual basis, or following any significant changes to FileLocal's operating environment.

This inventory is intended as a reference for FileLocal to use to track all FileLocal information assets (servers, laptops, etc), and should be updated on at least an annual basis, or following any significant changes to FileLocal's operating environment.

11.2 Inventory

Asset Name (ie, fully qualified	Location	Description/Purpose (including criticality	Party Responsible/Owner	Serial Number

For further details on any statement in this guide, please refer to the related policy or standard or ask your manager or information security representative

Public Records Policy

1. PURPOSE

   A. The purpose of this policy is to define public records and provide a procedure for the proper reporting and response to records requests.

   B. The Revised Code of Washington (RCW) 42.56, commonly known as the Public Records Act, requires public agencies to make identifiable, non-exempt public records available for inspection and copying upon request and to publish rules of procedure to inform the public how access to public records will be accomplished.

   C. In carrying out its responsibilities under the Act, FileLocal will be guided by the provisions of the Public Records Act describing its purposes and interpretation.

2. RESPONSIBILITY

   A. FileLocal's Program Manager and designated Public Records Officer

3. BACKGROUND

   A. FileLocal public records are available for public inspection and duplication, except as otherwise provided by RCW 42.56.001-42.56.904 or other statutes. All records will be released if they do not fall within the specific exemptions of the Public Records Act or other statutes which exempt or prohibit disclosure of specific information or records.

   B. The Public Records Act defines a public record as any "writing containing information relating to the conduct of government or the performance of any governmental or proprietary function prepared, owned, used or retained" by the agency.

   C. "Writing," broadly defined, means "handwriting, typewriting, printing, Photostatting, photographing, and every other means of recording any form of communication or representation, including, but not limited to, letters, words, pictures, sounds, or symbols, or combination thereof, and all papers, maps, magnetic or paper tapes, photographic films and prints, motion picture, film and video recordings, magnetic or punched cards, discs, drums, diskettes, sound recordings, and other documents including existing data compilations from which information may be obtained or translated." This includes emails, text messages, blogs, tweets and any emerging technologies used to conduct agency business.

   D. FileLocal makes many public records available on its website: FileLocal.org

   E. Original FileLocal records will not be permitted out of the FileLocal premises. Inspection of any public records shall be conducted in the presence of a Public Records Officer or designee. No public record may be marked, defaced, torn, damaged, destroyed, unreasonably disorganized, or removed from its proper location by order of a member of the public.

4. FILELOCAL PROCEDURES

   A. FileLocal's business office is located at 700 5th Avenue, Suite 4350. Seattle WA 98124.

   B. The FileLocal Public Records Officer is the Program Manager.

   C. All requests for public records must be directed in writing to the Public Records Officer and should specify that they are a request for public records under the state public records act. A public records request form will be provided on the FileLocal website.

   D. A set per-page charge of $0.15 will be assessed for 10 or more pages of black and white copies of letter or legal-sized pages (each side of a sheet is one page). If FileLocal has to pay an outside firm for duplicating records in non-routine formats such as photographs, blueprints or tape recordings, the actual costs will be passed along to the requestor.

   E. Before beginning to copy records, the Public Records Officer or designee may require a deposit of up to ten percent of the estimated costs of copying the records selected by a requestor. The Public Records Officer may also require the payment of the remainder of the copying costs before providing all of the records, or the payment of the costs of copying an installment before providing that installment. Payment may be made by check or money order to FileLocal.

   F. The Public Records Officer has the discretion to waive copying charges for small requests or for individuals or government agencies doing business with FileLocal if the Public Records Officer determines that this action is in the best interest of the agency.

   G. If possible, electronic records should be provided in their existing format, if requested in that format. However, if it necessary to burn files to a device the requestor may be charged $1.00 per CD or $10 per 16 GB thumb drive. When standard 8 ½ x 11 records are scanned from paper to .pdf, the requestor may be charged .10 cents per page.

5. RECORDS EXEMPT FROM DISCLOSURE

   A. After FileLocal has gathered responsive records, FileLocal will determine whether an exemption applies to all or part of the record.

   B. FileLocal is not required to permit public inspection and copying of records for which public disclosure of the record is prohibited or limited by state or federal statue or regulation. If any item is withheld, a written statement of the specific reasons will be provided by the Public Records Officer.

6. DELETION/REDACTION OF EXEMPT MATERIALS

   A. FileLocal is not relieved of its obligation to respond to requests for public records because a portion of the record contains information covered by an exemption. FileLocal has a duty to delete or redact specific information covered by an exemption and disclose the remainder of the record.

   B. If any item is withheld, a written statement of the specific reasons will be provided by the Public Records Officer.

7. MAKING A PUBLIC RECORDS REQUEST

   A. Contact information for FileLocal's Public Records Officer and procedures for making a public disclosure request are to be clearly identified on the FileLocal website – including the provision of an online form and/or PDF.

B. Requestors are encouraged to view the many documents available on the FileLocal website (www.FileLocal.org) prior to submitting a public records request.

C. Any person wishing to request access to public records or seeking assistance making a request should contact FileLocal's public records officer. The Public Records Officer oversees compliance with the Public Records Act, but may designate other staff who may process requests of public records.

D. The Public Records Officer may be reached at 700 5th Avenue, Suite 4350; P.O. Box 94669; Seattle WA 98124-4669; Jamie Carnell (Jamie.Carnell-FLO@seattle.gov) or phone 206-615-0493.

E. Persons making a public records request should include the following information, in writing:

I. Date and time of the request

II. Name of requestor

III. Contact information for the requestor

IV. Date range for the records requested

V. A detailed description of the requested records including the document name, if applicable.

8. PROCESSING OF PUBLIC RECORDS REQUESTS

A. Within five (5) business days from the receipt of the request, FileLocal must respond by:

I. Making the records available for inspection or copying; **OR**

II. If copies are requested and payment has been received, sending the copies to the requestor; **OR**

III. Acknowledgement of the receipt of the request and an estimate of additional time needed to produce the information requested; Additional time required to respond to a request may be based on the need to clarify the intent of the request, to locate and assemble information requested, to notify third persons or agencies affected by the request, or to determine whether any of the information requested is except and that a denial should be made to all or part of the request; **OR**

IV. Denial of the request and providing a written statement of specific reasons.

B. If FileLocal does not respond in writing within five business days of receipt of the request for disclosure, the requestor should consider contacting the Public Records Officer to determine the reason for the failure to respond.

C. When a records request is for a large volume of records, FileLocal may elect to provide the records on an installment basis.

9. RECORDS INSPECTION

A. Public records are available for inspection and copying during normal business hours (Monday through Friday 10 a.m. to 2 p.m., excluding legal holidays). The agency and requestor can make mutually agreeable arrangements for times of inspection and copying. Records must be inspected at the FileLocal offices.

B. FileLocal will maintain its records in a reasonably organized manner and will take reasonable actions to protect records from damage and disorganization. A requestor shall not take FileLocal records from the agency offices without the permission of the Public Records Officer or designee.

10. RECORDS INDEX

A. Compliance with RCW 42.17.260(3) is unnecessary, would be unduly burdensome and would interfere with FileLocal's implementation of an efficient, cost-effective business license and tax portal. The maintenance of detailed indexes is not practical or feasible and cannot be accomplished within the project schedule and budget because of limited staff resources, the voluminous amount of documents associated with the project, and the contract management approach to project development and operations.

11. RETENTION OF RECORDS

A. FileLocal is not required to retain all records it creates or uses. Retention schedules vary based on the content of the record. FileLocal will retain records in accordance with retention schedules approved by the State Local Records Committee. Public records may not be destroyed per a retention schedule if a public records request or actual or anticipated litigation is pending.

B. Because an electronic record is usually more susceptible to manipulation and alteration than a paper record, FileLocal will keep, when feasible, an electronic copy of the electronic records it provides to a requestor to be able to show the exact records it provided if necessary

C. FileLocal's records will be stored in a safe, secure, and accessible manner. Documents and financial files that are essential to keeping FileLocal operating in an emergency will be duplicated or backed up at least every week and maintained off-site.

D. FileLocal's Secretary is responsible for the ongoing process of identifying its records, which have met the required retention period, and overseeing their destruction. Destruction of financial and personnel-related documents will be accomplished by shredding.

E. Personal electronic devices, if used to conduct FileLocal business, will be subject to public disclosure. Failure on the part of employees to follow this policy can result in possible civil and criminal sanctions against FileLocal and its employees and possible disciplinary action against responsible individuals.

F. FileLocal's Program Manager will periodically review these procedures with FileLocal's legal counsel and certified public accountant to ensure that they are in compliance with new or revised regulations.

12. PUBLIC DISCLOSURE LOG

A. The FileLocal Public Disclosure Officer will maintain a log of all public disclosure requests including: tracking staff time and expenditures related to the responses to records requests and the request date, response date, closing date, requestor name, responsible parties, referrals to other departments, general subject of request, general information on redactions, and information on appeals and determinations.

13. PUBLIC DISCLOSURE TRAINING

    A. Training has been and will continue to be provided to all FileLocal Executive Board members and staff to create a culture of compliance within the organization.

14. DISCLAIMER OF LIABILITY

    A. This policy is not intended to expand or restrict the rights of disclosure of privacy as they exist under state and deferral law. Despite the use of any mandatory terms such as “shall” nothing in this policy is intended to impose mandatory duties on FileLocal beyond those imposed by the state and federal law.

15. ANNUAL REVIEW OF POLICIES BY EXECUTIVE BOARD

- The FileLocal Program Manager will review these policies on an annual basis

Use of Electronic Signatures

1. PURPOSE

To establish an electronic signature policy for FileLocal, under the authority of Section 18, Engrossed Substitute Senate Bill 6028, Chapter 57, Laws of 2020 (repealing and replacing Chapter 19.360 RCW), that:

- Promotes electronic transactions and removes barriers to conducting electronic transactions;
- Promotes efficiency in order to conserve public resources;
- Establishes guidelines for the use of electronic signatures for certain agency records and transactions;
- Controls the process for applying or obtaining signatures on agency resolutions and business records;
- Provides reasonable assurance of the integrity, authenticity, and nonrepudiation of documents when signed using electronic signatures; and
- Determines the scope of use of the current electronic signature platform provider (Adobe Sign) as the approved method for affixing an electronic signature to an electronic record. These policies will apply to any future replacement of the Adobe Sign platform.

Additionally, reducing FileLocal's reliance on paper-based transactions will further improve information security and sharing, allow faster approval of and access to documents, and reduce costs and environmental impacts.

2. DEFINITIONS

Authentication: The assurance that the electronic signature is that of the person purporting to sign the record or conduct the electronic transaction.

Electronic record: A record created, generated, sent, communicated, received, or stored by electronic means.

Electronic signature: An electronic sound, symbol, or process attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to authenticate or adopt the record.

Record: Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form, except as otherwise defined for the purpose of state or local agency record retention, preservation, or disclosure.

Sign: With present intent to adopt or authenticate a record, to execute or adopt a tangible symbol, or to attach to or logically associate with a record an electronic symbol, sound, or process.

Tangible medium: A writing, copy of a writing, facsimile, or a physical reproduction, each on paper or on other tangible material.

Wet Signature: A signature created when a person physically marks a document with a name or symbol, using a pen, seal, or similar writing instrument, with the intent to adopt or authenticate the record.

3. POLICY

A. An Electronic Signatures Recognized. FileLocal encourages electronic transactions and the use of electronic signatures. Filelocal recognizes electronic signatures as legally binding and equivalent in force and effect as wet signatures and authorizes the use and acceptance of electronic signatures as a substitute for wet signatures on agency records requiring or allowing signatures, except as provided herein or as otherwise required by law.

B. Persons Authorized to Use Electronic Signatures. The Program Manager, Chair and Vice Chair of the Executive Board, and their designees ("Authorized Persons") are authorized to sign agency records using any electronic signature platform approved under this policy to affix their electronic signatures to agency records as provided in this policy.

C. Adobe Sign Authorized. The Adobe Sign electronic signature platform, and any future replacement of the Adobe Sign platform, is hereby approved and authorized for use in affixing electronic signatures of Authorized Persons to all agency records for which an electronic signature is required or permitted under this policy.

D. Desired-Signature Transactions: Electronic signatures may be used when a valid written or electronic signature is not required by law, regulation, or agency policy but is desired to emphasize the significance or importance of a record or transaction ("Desired-Signature Transactions"). In these cases, there is no legal requirement for authentication, and a signature method other than Adobe Sign is authorized (i.e. use of digital image of signature). Examples of Desired-Signature Transactions include, but are not limited to, memos, correspondence, meeting minutes, time sheets, and approved claims vouchers. Adobe Sign or a wet signature may be used for such documents, but it is not required.

E. Required-Signature Transactions: Electronic signatures may be used by Authorized Persons when law, regulation, or agency policy requires a record or transaction to have a valid signature before it is considered legally effective ("Required-Signature Transactions"). Required-Signature Transactions include, but are not limited to, contracts, offer letters, and Executive Board resolutions. In these cases, the signature method must be Adobe Sign, or a replacement platform that is equally capable of secure authentication of the signer.

F. Executive Board Resolutions: For resolutions approved by the Executive Board, an electronic copy of the resolution will be provided by the Program Manager or designee to the authorized signatory for that person to sign. For electronic signatures, the authorized signatory shall sign

the resolution as a Required-Signature Transaction under this policy and return it to the Program Manager or designee for retention.

G. Wet Signatures Authorized. This policy in no way affects FileLocal's ability to sign a record or conduct a transaction using a physical medium and shall not be construed as a prohibition on the use of wet signatures.

H. Changes to this Policy. This policy may be amended, rescinded, or replaced at any time by the Executive Board, except that the Program Manager is authorized to substitute a different electronic signature platform that, in his or her discretion, has equal or better security, integrity, and auditability features as Adobe Sign.

KEY GOVERNANCE DOCUMENTATION

The Washington Multi-City Business License and Tax Portal (dba FileLocal) was formed in March 2014 under an Interlocal Agreement and Related Articles of Incorporation.

The agency is organized as a public body and instrumentality of its members to jointly exercise essential governmental functions of its members in accordance with the Interlocal Cooperation Act (39.34 RCW), which permits a local government to enter into interlocal agreements with other public agencies in the interest of cooperatively sharing resources for their mutual benefit.

FileLocal's Articles of Incorporation are filed with the Washington Secretary of State and are the primary rules governing the management of the enterprise. Key documentation included in Appendix A:

1. Articles of Incorporation
2. Interlocal Agreement
3. Bylaws



ARTICLES OF INCORPORATION

APPENDIX NO. A1

ARTICLES OF

INCORPORATION OF

WASHINGTON MULTI-CITY BUSINESS LICENSE AND TAX PORTAL AGENCY

The undersigned, in order to form a not for profit corporation under Chapter 24.06 of the Revised Code of Washington ("RCW"), and pursuant to Chapter 39.34 RCW, hereby sign and deliver the following Articles of Incorporation:

ARTICLE I — NAME

The name of this corporation is:

WASHINGTON MULTI-CITY BUSINESS LICENSE AND TAX PORTAL AGENCY

ARTICLE II — DURATION

The period of duration of Washington Multi-City Business License and Tax Portal Agency (the "PORTAL AGENCY") is perpetual.

ARTICLE III — PURPOSES

PORTAL AGENCY is organized on behalf of and as an instrumentality of its governmental members to carry out certain exclusively governmental activities and the purposes of the Washington Multi-City Business License and Tax Portal Agency Interlocal Agreement (the "Interlocal Agreement") pursuant to the Interlocal Cooperation Act, Chapter 39.34 RCW. These purposes include developing, owning, operating and managing and maintaining an internet web application gateway to administer City business licensing and tax collection functions (the "Portal"), as further described in the Interlocal Agreement.

ARTICLE IV — PROHIBITED ACTIVITY

Notwithstanding any of the provisions of these Articles of Incorporation, the PORTAL AGENCY shall not conduct or carry on activities not permitted to be conducted or carried on by an organization exempt from federal income tax under Sections 115 of the Internal Revenue Code or by an organization, contributions to which are deductible under Section 170(c)(2). No part of the net earnings of the PORTAL AGENCY shall inure to the benefit of any director,

officer or private individual. No substantial part of the activities of the PORTAL AGENCY shall be devoted to the carrying on of propaganda, or otherwise attempting to influence legislation except as may be permitted by the Internal Revenue Code, and the PORTAL AGENCY shall not participate in, or intervene in (including the publication or distribution of statements regarding) any political campaign on behalf of or in opposition to any candidate for public office. The PORTAL AGENCY

shall not have or issue shares of stock, shall not make any disbursement of income to its directors or officers, and shall not make loans to its officers or directors.

ARTICLE V — POWERS

In general, and subject to such limitations and conditions as are or may be prescribed by law, or in these Articles of Incorporation or in the PORTAL AGENCY'S Bylaws or in the Interlocal Agreement, the PORTAL AGENCY shall have all powers which now or hereafter are conferred under Chapters 24.06 and 39.34 RCW and other applicable law upon a corporation organized for the purposes set forth above, or are necessary or incidental to the powers so conferred, or are conducive to the attainment of the PORTAL AGENCY's purposes.

ARTICLE VI — MEMBERS

Each Member of PORTAL AGENCY must be a general-purpose municipal corporation formed and existing as a city or town under the laws of the state of Washington and meeting the other requirements described in the Interlocal Agreement. As used in these Articles, the term "Members" means "Principals" as defined in the Interlocal Agreement. The rights and responsibilities of the Members/Principals and the manner of their election, appointment, or admission to membership and termination of membership shall be as provided for in the Interlocal Agreement. The PORTAL AGENCY shall have one class of Members/Principals, except that each Member/Principal may be treated as a separate class for calculating votes as provided for in the Interlocal Agreement.

ARTICLE VII — DISTRIBUTIONS UPON DISSOLUTION

No director, trustee or officer of the PORTAL AGENCY, nor any private individual, shall be entitled to share in the distribution of any of the corporate assets upon dissolution of the PORTAL AGENCY or the winding up of its affairs. Upon dissolution of the PORTAL AGENCY, after paying, satisfying, and discharging, or making adequate provision therefor, of all liabilities and obligations of the PORTAL AGENCY, and after returning, transferring, or conveying assets held by the PORTAL AGENCY requiring return, transfer, or conveyance on condition of the dissolution, all remaining assets of the PORTAL AGENCY shall be distributed by the Executive Board as provided for in the Interlocal Agreement.

ARTICLE VIII — DISSENTING MEMBERS

"Dissenting members," as that term is used in RCW 24.06.245 through 255, will be entitled to the rights and allocation of assets set forth in the Interlocal Agreement, but may be limited to "a return of less than the fair value" of their membership as that term is used in RCW 24.06.255.

ARTICLE IX — BYLAWS

Provisions for the regulation of the internal affairs of the PORTAL AGENCY shall be set forth in the Bylaws of the PORTAL AGENCY.

ARTICLE X — REGISTERED AGENT

The address of the initial registered office of the PORTAL AGENCY is 600 4th Avenue Seattle WA 98104. The name and address of its initial registered agent is Glen Lee, Finance Director, City of Seattle, 700 Fifth Avenue, Suite 4350, Seattle, WA 98104.

ARTICLE XI — DIRECTORS

The initial board of directors (referred to in the Interlocal Agreement as the "Executive Board") shall consist of four (4) directors. The names and addresses of the persons who are to serve as initial directors are:

Ms. Jan Hawn, Finance Director
City of Bellevue
450 110th Avenue N.E.
Bellevue, WA 98004

Ms. Debra Bryant, Chief Finance Director
City of Everett
2930 Wetmore Avenue
Everett, WA 98201

Mr. Glen Lee, Finance Director
City of Seattle
700 Fifth Avenue, Suite 4350
Seattle, WA 98104

Mr. Andy Cherullo, Finance Director
City of Tacoma
747 Market Street
Tacoma, WA 98402

Directors may be removed as provided for in the Bylaws.

ARTICLE XII -- OFFICERS

The PORTAL AGENCY shall have four officers, a President, Vice-President, Secretary and

Treasurer. The President and Vice-President are referred to as the "Chair" and Vice-Chair" respectively, in the Interlocal Agreement. The responsibilities of the officers shall be described in the PORTAL AGENCY Bylaws.

ARTICLE XIII — INCORPORATORS

The names and addresses of the incorporators are:

1. City of Bellevue
   450 110th Avenue N.E.
   Bellevue, WA 98004

2. City of Everett
   2930 Wetmore Avenue
   Everett, WA 98201

3. The City of Seattle
   600 4th Avenue
   Seattle, WA
   98104

4. City of Tacoma
   747 Market Street
   Tacoma, WA
   98402

ARTICLE XIV — LIMITATION OF DIRECTOR LIABILITY

Except to the extent otherwise required by applicable law (as it exists on the date of the adoption of this Article or may be amended from time to time), a director of the PORTAL AGENCY (a director is referred to as a "Member of the Executive Board" in the Interlocal Agreement) shall not be personally liable to the PORTAL AGENCY for monetary damages for conduct as a director, except for liability of the director (i) for acts or omissions which involve intentional misconduct by the director or a knowing violation of law by the director, (ii) for any transaction from which the director will personally receive a benefit in money, property or services to which the director is not legally entitled, or (iii) for any act or omission occurring before the date when this provision becomes effective.

If the Washington Nonprofit Miscellaneous and Mutual Corporation Act (the "Act") I hereafter amended to expand or increase the power of the PORTAL AGENCY to eliminate or limit the personal liability of directors, then, without any further requirement of action by the directors of the PORTAL AGENCY, the liability of a director shall be eliminated or limited to the full extent permitted by the Act. No amendment to or repeal of this Article shall adversely affect any right of protection of any director of the PORTAL AGENCY occurring after the date of the adoption of this Article and prior to such amendment or repeal.

ARTICLE XV — INDEMNIFICATION

Except as provided in Article XIV, the PORTAL AGENCY shall indemnify any director and officer of the PORTAL AGENCY who is involved in any capacity in a proceeding (as defined in RCW 23B.08.500, as presently in effect and as hereafter amended) by reason of the position held by such person or entity in the PORTAL AGENCY to the full extent allowed by law, as presently in effect and as hereafter amended. By means of a resolution or of a contract specifically approved by the Board of Directors (referred to as the "Executive Board" in the Interlocal Agreement), the PORTAL AGENCY may also indemnify an employee, or agent to such degree as the Board of Directors determines to be reasonable, appropriate, and consistent with applicable law and to be in the best interests of the PORTAL AGENCY. Reasonable expenses incurred by a director or officer who is involved in any capacity in a proceeding by reason of the position held in the PORTAL AGENCY, shall be advanced by the PORTAL AGENCY to the full extent allowed by and on the conditions required by applicable law, as presently in effect and as hereafter amended.

The Board of Directors of the PORTAL AGENCY shall have the right to designate the counsel who shall defend any person or entity who may be entitled to indemnification, to approve any settlement, and to approve in advance any expense. The rights conferred by or pursuant to this Article shall not be exclusive of any other rights that any person may have or acquire under any applicable law (as presently in effect and as hereafter amended), these Articles of Incorporation, the bylaws of the PORTAL AGENCY, a vote of the Board of Directors of the PORTAL AGENCY, or otherwise. No amendment to or repeal of this Article shall adversely affect any right of any director, officer, employee, or agent for events occurring after the date of the adoption of this Article and prior to such amendment or repeal.

The PORTAL AGENCY shall also indemnify and hold harmless every Member/Principal, including, but not limited to that Member's/Principal's officers, directors, employees and agents from all claims, injuries, damages, losses or suits, including reasonable attorney fees which arise out of acts and/or omissions of the PORTAL AGENCY. To such degree as the board of directors/Executive Board determines to be reasonable, appropriate, and consistent with applicable law and to be in the best interests of the PORTAL AGENCY, the PORTAL AGENCY may also indemnify and hold harmless Subscribers, including, but not limited to that Subscriber's officers, directors, employees and agents from all claims, injuries damages, losses or suits, including reasonable attorney fees which arise out of acts and/or omissions of the PORTAL AGENCY.

Nothing in these Articles of Incorporation may be interpreted as a waiver of sovereign immunity by any member.

Indemnification of directors and officers by the PORTAL AGENCY shall be consistent with the terms of the Interlocal Agreement, the Act, the Interlocal Cooperation Act and other applicable Jaw. In the event of any inconsistency between this Article and the lnterlocal Agreement, the terms of the Interlocal Agreement shall control to the extent consistent with applicable law.

Notwithstanding any other provision of this Article, no indemnification shall be provided to any person if in the reasonable opinion of competent counsel, payment of such indemnification would cause the PORTAL AGENCY to lose its exemption from federal income taxation.

DATED as of this 1st day of March 2014.

INCORPORATORS:

INCORPORATOR: City of Bellevue

By: Interim City Manager Brad Miyake

INCORPORATOR: The City of Seattle

by: Mayor Edward B. Mu1Tay

INCORPORATOR: City of Everett

By: Mayor Ray Stephanson

INCORPORATOR: City of Tacoma

by: City Manager T.C. Broadnax

Indemnification of directors and officers by the PORTAL AGENCY shall be consistent with the terms of the lnterlocal Agreement, the Act, the Interlocal Cooperation Act and other applicable law. In the event of any inconsistency between this Article and the lnterlocal Agreement, the terms of the Interlocal Agreement shall control to the extent consistent with applicable law.

Notwithstanding any other provision of this Article, no indemnification shall be provided to any person if in the reasonable opinion of competent counsel, payment of such indemnification would cause the PORTAL AGENCY to lose its exemption from federal income taxation.

DATED as of this 1st day of March 2014.

INCORPORATORS:

INCORPORATOR: City of Bellevue

By: Interim City Manager Brad Miyake

INCORPORATOR: The City of Seattle

by: Mayor Edward B. Murray

INCORPORATOR: City of Everett

By: Mayor Ray Stephanson

ATTEST:

City Clerk

INCORPORATOR: City of Tacoma

By: City Manager T.C. Broadnax

Indemnification of directors and officers by the PORTAL AGENCY shall be consistent with the tem1s of the Interlocal Agreement, the Act, the Interlocal Cooperation Act and other applicable law. In the event of any inconsistency y between this Article and the Interlocal Agreement, the terms of the Interlocal Agreement shall control to the extent consistent with applicable Jaw.

Notwithstanding any other provision of this Article, no indemnification shall be provided to any person if in the reasonable opinion of competent counsel, payment of such indemnification would cause the PORTAL AGENCY to lose its exemption from federal income taxation.

DATED as of this 1st day of March 2014.

JNCORPORATORS:

JNCORPORATOR: City of Bellevue

By: Interim City Manager Brad Miyake

INCORPORATOR: The City of Seattle

By: Mayor Edward B. Murray

INCORPORATOR: City of Everett

By: Mayor Ray Stephenson

INCORPORATOR: City of Tacoma

by: City Manager T.C. Broadnax

Indemnification of directors and officers by the PORTAL AGENCY shall be consistent with the terms of the Interlocal Agreement, the Act, the Interlocal Cooperation Act and other applicable law. In the event of any inconsistency between this Article and the Interlocal Agreement, the terms of the Interlocal Agreement shall control to the extent consistent with applicable law.

Notwithstanding any other provision of this Article, no indemnification shall be provided to any person if in the reasonable opinion of competent counsel, payment of such indemnification would cause the PORTAL AGENCY to lose its exemption from federal income taxation.

DATED as of this 1st day of March 2014.

INCORPORATORS:

INCORPORATOR: City of Bellevue

By: Interim City Manager Brad Miyake

INCORPORATOR: The City of Seattle

by: Mayor Edward B. Munday

INCORPORATOR: City of Everett

By: Mayor Ray Stephenson

INCORPORATOR: City of Tacoma

By: City Manager T.C. Broadnax



INTERLOCAL AGREEMENT

APPENDIX NO. A2

WASHINGTON MULTI-CITY BUSINESS LICENSE AND TAX PORTAL AGENCY INTERLOCAL AGREEMENT

BY AND BETWEEN THE CITIES OF

BELLEVUE

EVERETT

SEATTLE

and

TACOMA

DATED AS OF MARCH 1, 2014

TABLE OF CONTENTS

Section	Caption	Page
	Recitals……	1
1	Creation of Washington Multi-City Business License and Tax Portal Agency….	2
2	Term of Agreement……	2
3	Definitions……....	3
4	Guiding Principles and Goals…….	6
5	Portal Agency Services……...	8
6	Portal Agency Powers…….	10
7	Executive Board: Composition and Operation……...	11
8	Conversion of Status of Participating Cites; Addition of New Principals or Subscribers……..	15
9	Tax and Finance Operations Committee…….	16
10	Portal Agency Staffing……	17
11	Portal Agency Manager……...	18
12	Assignment of Portal Services Contract from Seattle to Portal Agency……	19
13	Budget; Cost Allocation; Capital Cost Recovery Charges; Payment of Charges; Delinquencies; Reserve Funds……	19
14	Retained Authority and Responsibility of Participating Agencies…….	23
15	Ownership of Property……	23
16	Merger or Consolidation, or Sale of All or Substantially All Assets……..	24
17	Withdrawal by, or Termination of, a Principal……...	24
18	Amendment of Agreement…….	25
19	Termination of Agreement; Dissolution of Agency……	25
20	Dispute Resolution……..	26
21	Insurance……	27
22	Indemnification and Hold Harmless……...	27
23	Intergovernmental Cooperation……..	28
24	Notice……..	29
24	Venue……..	29
26	Filing……...	29
27	No Third-Party Beneficiaries……..	29
28	Severability…….	30
29	Ratification……..	30
30	Execution, Counterparts and Effective Date……...	30
	List of Exhibits……...	32
A	Proposed 2014 Portal Agency Budget Summary……..……...	33
B	2015-2020 Estimated Portal Agency Operating Budget Summary……	35
C	Capital Cost Recovery Charges…….....	37
D	Calculation of New Participant Capped Cost Increment and New Participant Labor Cost Increment……...	38

WASHINGTON MULTI-CITY BUSINESS LICENSE AND TAX PORTAL AGENCY INTERLOCAL AGREEMENT

THIS AGREEMENT, incorporating all exhibits hereto, is entered into by and between the Cities of Bellevue, Everett, Seattle and Tacoma (collectively, the "Principals") pursuant to the Interlocal Cooperation Act Ch. 39.34 RCW and has been authorized by the legislative body of each Principal.

RECITALS

WHEREAS, each of the Principals is a city, a general-purpose municipal corporation authorized by state law to issue local business licenses and collect a variety of local taxes; and

WHEREAS, the Principals seek to make it easier and more efficient for businesses to apply for local business licenses and file local taxes, while retaining local control over local licensing and tax collection functions and policies; and

WHEREAS, the Principals seek to accomplish these goals by jointly facilitating the creation of an internet web application gateway (the "Portal") where tax collection and business licensing functions can be collectively administered, and where businesses operating in multiple cities can use a "one-stop" system for tax payment or business license application filing; and

WHEREAS, the Principals have engaged in extensive outreach with other cities, state legislators, taxpayers and the business community to understand the interests of these stakeholders in relation to development of the Portal; and

WHEREAS, the creation of an intergovernmental entity, in the form of a governmental nonprofit corporation whose members are Principals to oversee the operation of the Portal will enable each Principal to participate in management of the Portal, provide economies of scale to participating cities, and ensure continued control by each Principal of its tax and licensing policy and local tax collections; and

WHEREAS, the collection of local taxes is an exclusively governmental activity of each of the cities party to this Agreement; and

WHEREAS, the creation of an intergovernmental entity as described in this Agreement will enable the Principals to carry out this exclusively governmental activity as a joint instrumentality; and

WHEREAS, it is anticipated that additional cities will elect to use the Portal over time, and that some may wish to do so as subscribers of the Portal's services rather than as principals; and

WHEREAS, The City of Seattle has provided start-up funding for the development of the Portal and has conducted a competitive procurement process in which staff from each of the Principals participated with Seattle staff in selecting a preferred vendor to provide portal development, hosting and maintenance services; and

WHEREAS, The City of Seattle has entered into a contract with the preferred vendor, and the vendor has begun work to develop the Portal with continued input from staff from each of the Principals;

NOW THEREFORE, in consideration of the promises and agreements contained in this Agreement and subject to the terms and conditions set forth, it is mutually understood and agreed by the Parties as follows:

SECTION 1. CREATION OF WASHINGTON MULTI-CITY BUSINESS LICENSE AND TAX PORTAL AGENCY.

The Washington Multi-City Business License and Tax Portal Agency, ("PORTAL AGENCY") is hereby created as authorized by the Interlocal Cooperation Act (Ch. 39.34 RCW), and shall be a municipal instrumentality of the Principals, jointly organized by the Principals as a nonprofit corporation under Chapter 24.06 RCW as expressly authorized by RCW 39.34.030(3)(b). The Principals each assign to PORTAL AGENCY the responsibility for overseeing the development, operation and maintenance of an internet web application gateway to administer city business licensing and tax collection functions as exclusively governmental activities, all as described herein.

SECTION 2. TERM OF AGREEMENT.

This Agreement shall have an initial term of approximately five years, ending on December 31, 2019, (the "Initial Term"), and shall thereafter be perpetual, subject to the termination provisions in Section 19 of this Agreement. During the Initial Term no Principal may withdraw from the Agreement, provided that a Principal may convert or be converted to Subscriber status as provided in Sections 8.a, 13.d and 13.k, and may upon action of the Executive Board be terminated from participation in the Agreement as provided in Section 13.k.

SECTION 3. DEFINITIONS.

a. Agreement. The "Agreement" is this interlocal agreement, as it may hereafter be amended or modified, together with all exhibits and appendices hereto, as they may hereafter be amended or modified.

b. Articles of Incorporation. The "Articles of Incorporation" or "Articles" are terms defining aspects of the PORTAL AGENCY corporate formation under 39.34.030(3)(b) and consistent with RCW 24.06.025, as they may hereafter be amended by the Executive Board.

c. Board Member. A "Board Member" or "Executive Board Member" is the individual representing a Principal on the Executive Board, whether the Chief Financial Officer of such Principal or his/her designated alternate.

d. Business and Occupation Taxes. "Business and Occupation Taxes" are Gross Receipt Taxes imposed by a Participating City as an exclusively governmental activity authorized by state law and as defined in RCW 35.102.030.

e. Business Licenses. "Business Licenses" are licenses required to be obtained by businesses in order to operate within a Participating City, consistent with state law.

f. Bylaws. "Bylaws" as adopted and amended from time to time by the Executive Board shall govern the operations of the PORTAL AGENCY Executive Board, Operations Committee, and the officers thereof.

g. Capital Cost Recovery Charge. The "Capital Cost Recovery Charge" is an annual fee charged to all Participating Cities other than the City of Seattle, for the purposes of reimbursing Seattle for a portion of the funding it provided to pay for start-up of the PORTAL AGENCY, as further described in Section 13.j.

h. Capped Costs. "Capped Costs" means all items in the PORTAL AGENCY budget *excluding*:

i. Labor Costs unrelated to increases in full or partial staff positions;
ii. Costs payable pursuant to the Portal Services Contract with the Vendor;
iii. State Auditor's Office Audit costs;
iv. Accounting services;
v. Insurance;
vi. Bank fees;
vii. Any unanticipated expenses outside the normal course of business, for example, costs of litigation or damages, uninsured losses, tax or other liabilities resulting from a change in law, and events of force majeure (e.g. fire, explosion, accident, volcanic eruption, flood, epidemic, civil disturbance).

i. CPI-U Limit. "CPI-U Limit" means the percentage increase (or decrease) equal to the percentage increase (or decrease) year to year in the Consumer Price Index – Urban for the Seattle/ Tacoma/Bremerton metropolitan area, April –April, calculated by the Federal Bureau of Labor Statistics, or its successor index.

j. Executive Board. The "Executive Board" is the body described in Section 7 and shall be the governing body of the PORTAL AGENCY.

k. Gross Receipts Taxes. "Gross Receipts Taxes" are taxes imposed by Participating Cities which are based on the gross receipts of certain businesses, specifically to include Business and Occupation Taxes as defined by RCW 35.102.030 as well as other taxes imposed by Participating Cities on utilities or businesses that are collected on basis of such gross receipts in accordance with applicable law. For purposes of this Agreement, Gross Receipts Taxes also includes square footage taxes imposed by a Participating City for the act or privilege of doing business in that city and calculated based on the amount of space occupied and used for those business activities within that city.

l. Initial Term. The "Initial Term" is the period from the effective date of this Agreement through December 31, 2019.

m. Labor Costs. "Labor Costs" include salary, benefits and other compensation provided to Portal Agency employees (if any) and/or loaned staff.

n. Licensees. "Licensees" are businesses or individuals that apply for a Business License from a Participating City or Cities using the Portal.

o. Manager. The "Manager" is the chief operating officer for PORTAL AGENCY appointed by and serving at the pleasure of the Executive Board.

p. New Participant Capped Cost Increment. The "New Participant Capped Cost Increment" is an amount calculated each budget period to identify the maximum amount by which Capped Costs may increase in the Executive Board approved draft or final budget for such period without unanimous approval of the Executive Board Members representing all Original Principals, as further described in Section 13.b.iv.1 and Exhibit D.

q. New Participant Labor Cost Increment. The "New Participant Labor Cost Increment" is an amount calculated each budget period to identify the maximum amount by which Labor Costs may increase to provide for additional full or partial staff positions in the Executive Board approved draft or final budget for such period without requiring unanimous approval of the Executive Board Members representing all Original Principals, as further described in Section 13.b.iv.2 and Exhibit D.

r. Operations Committee. The "Operations Committee" or "Tax and Finance Operations Committee" is the committee described in Section 9.

s. Original Principals. The Original Principals are those four cities initially signing this Agreement: the cities of Bellevue, Everett, Seattle and Tacoma.

t. Participating Cities. All Principals, and all Subscribers, as they may be so constituted from time to time, are collectively referred to as the "Participating Cities" or "Participants," and individually referred to as a "Participating City" or "Participant."

u. Population. "Population" is the residential population of a City, according to the most recent annual report issued by the State Office of Financial Management each year determining the population of each city for purposes of taxation and allocation of certain state shared revenues in the following calendar year.

v. Portal. The "Portal" is an internet web application gateway owned, operated and maintained by the Vendor under contract with the PORTAL AGENCY that affords Taxpayers and businesses a single access point through which they may apply for business licenses from, and pay taxes and fees to, Participating Cities, and receive information related to these functions.

w. PORTAL AGENCY. "PORTAL AGENCY" means the Washington Multi-City Business License and Tax Portal Agency.

x. Portal Operations Policy. The "Portal Operations Policy" is a separate document adopted by Supermajority Vote of the Executive Board, as it may be amended from time to time, which describes how data will be shared between the Participating Cities and the PORTAL AGENCY, and sets forth operating procedures and rules for the Portal.

y. Portal Services Contract. The 'Portal Services Contract" is that certain contract dated as of September 6, 2013 between The City of Seattle and Avenu Systems, a Louisiana corporation, to develop software for, and host the Portal operations. The Portal Services Contract is to be assigned to the PORTAL AGENCY by The City of Seattle pursuant to Section 12 of this Agreement.

z. Principal. A "Principal" is a general purpose municipal corporation formed as a city under the laws of the state of Washington which imposes a Business and Occupations Tax and which has accepted the terms of and is a party to this Agreement and has paid its share of initial costs as may be required by the Executive Board as a condition to becoming a Principal. Principals shall receive services offered by the PORTAL AGENCY according to such terms and conditions as may be established by the Executive Board.

aa. Representative. The term "Representative" refers to the individual representing a Principal or a Subscriber on the Operations Committee, or his/her designated alternate.

bb. Simple Majority Vote. A "Simple Majority Vote" of the Executive Board means a majority (more than 50%) of the votes of the Board Members present constituting a quorum, with each Board Member that is present and voting having one vote.

cc. Subscriber. A "Subscriber" is a general purpose municipal corporation, formed as a city under the laws of Washington which has agreed to pay the PORTAL AGENCY for services according to such terms and conditions as may be established by the Executive Board and evidenced by separate contract between the PORTAL AGENCY and such entity. A Principal may convert or be converted to Subscriber status as provided in Sections 8, 13.d and 13.k and a Subscriber may convert to a Principal as described in Section 8.

dd. Supermajority Vote. A "Supermajority Vote" means Executive Board approval of an item accomplished by securing affirmative votes of not less than sixty-six percent (66%) of all voting Board Members of the Executive Board in number, and not less than sixty-six percent (66%) in number of the Original Principals.

ee. Taxpayers. "Taxpayers" are businesses subject to local city taxes imposed by a Principal or Subscriber, payment of which is or can be administered by the Portal.

ff. Transaction. A "Transaction" is a payment or filing for a Business License, or a payment or filing of an online tax form (where multiple taxes filed on the same online tax form are counted as a single Transaction), made on the Portal by a business to a Participating City; *provided, however,* that where historical actual Transactions counts are to be used (rather than payments and transactions made *on the Portal*), then Transactions includes the total actual Business License filings and Gross Receipts Tax filings (where multiple taxes filed on the same tax form are counted as a single Transaction) for the Participating City over the applicable period. The Executive Board may refine this definition from time to time by amending the Portal Operations Policy in order to accommodate expansion of services offered by the Portal or to address other issues.

gg. User Fees. "User Fees" are fees and charges imposed on businesses, Licensees or Taxpayers per Executive Board approval as part of PORTAL AGENCY's budget approval process.

hh. Vendor. The Vendor is Avenu Systems, a Louisiana corporation, which through the Portal Services Contract is providing services to develop, establish, host, own and maintain the Portal, associated online data storage and services. The Vendor has ownership of the Portal. The term Vendor shall also include any successor in interest to Avenu Systems or any successor firm(s) or agency(s) with which the PORTAL AGENCY may contract to provide Portal development, hosting, maintenance, and associated online data storage and services.

SECTION 4. GUIDING PRINCIPLES AND GOALS.

a. Guiding Principles of PORTAL AGENCY. The Principals intend that the PORTAL AGENCY actions be guided by the following guiding principles:

i. Local Control – The PORTAL AGENCY will seek to respect and preserve each Participating Cities' authority to set local tax policies.

ii. Integrity – The PORTAL AGENCY will be honest, truthful and straightforward.

iii. Accountability – The PORTAL AGENCY will be responsible for its actions and decisions, a good steward of public funds and transparent in its operations.

iv. Flexibility / Adaptability – The PORTAL AGENCY will strive to nimbly respond to a changing business, technology and policy environment.

v. Security – The PORTAL AGENCY will at all times seek to safeguard Taxpayer, Licensee and Participating City data.

vi. Accessibility – The PORTAL AGENCY will seek to be accessible and responsive to Taxpayers, Licensees and Participating Cities.

vii. Affordability – The PORTAL AGENCY will seek to be affordable to both Participating Cities and businesses and taxpayers using the Portal. Also, fees

and charges will be structured so that the addition of new Cities using the Portal does not impose additional costs on prior Participating Cities.

b. Goals of the PORTAL AGENCY. The Principals acknowledge and support the following goals which they seek to accomplish by this Agreement and creation of the PORTAL AGENCY:

i. Taxpayers and Licensees utilizing the Portal will have a seamless, transparent, user-friendly and efficient experience.

ii. It will be easy and timely for Taxpayers and Licensees to access knowledgeable staff at each Participating City to respond to tax or licensing questions.

iii. The Portal will have error-free data collection, transmittal and tax payment allocation as between Participating Cities.

iv. There will be local control and oversight of tax collections and tax policy.

v. Participating Cities will be accountable for the accuracy and timeliness of information they provide to the PORTAL AGENCY and for their customer service response.

vi. Decision-making will by jointly exercised by the Principals through the Executive Board.

vii. The PORTAL AGENCY will seek to balance the interests of information technology, treasury, finance and tax staff within Participating Cities in the development of the Portal's capabilities and operating rules.

viii. The PORTAL AGENCY will comply with all legal requirements, including but not limited to public record-keeping, public meetings, public records, security, and audit requirements.

ix. The PORTAL AGENCY will be able to accommodate additional city partners as Principals or Subscribers over time and be able to process additional types of local taxes and licenses over time.

x. The PORTAL AGENCY will support the ability to maximize use of the Portal by Taxpayers and Licensees so that Participating Cities do not need to replicate the Portal's services.

xi. The PORTAL AGENCY will maximize compatibility with Participating City's systems of record for data storage and processing.

xii. The PORTAL AGENCY will coordinate with the state Department of Revenue.

xiii. The PORTAL AGENCY will be a cost-effective solution for Participating Cities.

SECTION 5. PORTAL AGENCY SERVICES.

a. Generally. The PORTAL AGENCY has the responsibility and authority for overseeing the Vendor's contractual responsibilities to develop, own, operate, maintain and manage the Portal and for managing the operations of the PORTAL AGENCY. It is expressly contemplated that this scope of services includes:

i. The implementation, operation and maintenance of replacement or upgrades of the Portal as necessary or appropriate.

ii. The development and adoption of rules for access, use and maintenance of the Portal by City Participants, Taxpayers and Licensees.

iii. Expansion of the scope of services offered through the Portal if approved per Subsection 5.c below.

iv. Other responsibilities reasonably necessary for the development, operation and maintenance of the Portal.

v. Other related or ancillary services.

b. Limitation on Authority. The PORTAL AGENCY shall have no authority to set tax rates or tax classifications for Participating Cities, to set local tax policy, tax rules, deductions or exemptions; or take enforcement action on behalf of any Participating City. The PORTAL AGENCY is created by the Principals to manage the Participating Cities' joint participation in the facilitation of an exclusively governmental activity, specifically, the collection of certain local taxes.

c. Expansion of Scope of Services. The Portal will be initially established with the capability to handle payment of Gross Receipts Taxes and filing of applications for Business Licenses. PORTAL AGENCY may provide additional capability to pay additional types of city taxes or application for additional types of city licenses through the Portal only upon approval of a Supermajority Vote of the Executive Board; *provided, however,* that the cost of service expansions will be allocated only to those Participating Cities electing to participate in such services.

d. Requirement of Participating Cities to Utilize Services of Portal**.**

i. Gross Receipts Tax Collection Services: Participating Cities shall be required to offer their Taxpayers the option of paying Gross Receipts Taxes through the Portal, if and to the extent such taxes are imposed by a Participating City.

ii. Other Services: Except as required by Subsection 5.d.i above, no Participating City shall be required to utilize any other service of the Portal without the prior written approval of such City.

iii. Provision of Alternate Collection Options by Participating Cities. Nothing in this Agreement shall be interpreted to preclude a Participating City from

offering its Taxpayers or businesses additional means (other than through the Portal) for acquiring Business Licenses or paying any local taxes, including but not limited to payment of Gross Receipts Taxes.

iv. Operating Policies and Rules for Use of Portal. In order to protect sensitive Taxpayer data and assure the relationship between the Portal and Participating Cities remains fully functional and secure, the Executive Board shall adopt a Portal Operations Policy. It is understood and agreed that the access and use of the Portal by any Principal or Subscriber is conditioned on that party consenting in writing to comply with the Portal Operations Policy. Such consent shall be signified by signature of the chief executive officer of each Participating City, or his/her designee, and shall not require further legislative action of the Participating City. The Portal Operations Policy will be regularly reviewed and updated by the Executive Board as necessary or appropriate.

e. Additional Activities of the PORTAL AGENCY. At the discretion of the Executive Board, the PORTAL AGENCY may, in addition to the services described in Section 5.a above:

i. Participate in forums for Participating Cities to discuss tax policy issues (including but not limited to the Association of Washington Cities Tax Policy Advisory Group or its successor in interest);

ii. Provide education to Taxpayers and Businesses regarding the Portal and the PORTAL AGENCY, and work to increase transparency about Participating City tax policies and activities;

iii. Provide a forum for businesses and others to provide feedback and suggestions on the use and functionality of the Portal and the taxes and licenses administered through the Portal; and

iv. Provide a forum for discussion, coordination and execution of coordinated enforcement activities, provided that the PORTAL AGENCY itself is not authorized to take any tax collection or license fee enforcement actions on behalf of a Participating City. The PORTAL AGENCY shall not use or authorize the use of the Portal or such forum for the purpose of assisting a campaign for election of any person to any office or for the promotion of or opposition to any ballot proposition.

v. The PORTAL AGENCY shall coordinate with the Washington State Department of Revenue with regard to the Portal's operations and functionality to minimize the need for Taxpayers and Licensees to enter data on the Portal and any separate state tax payment and licensing systems.

SECTION 6. PORTAL AGENCY POWERS.

Through its Executive Board**,** the PORTAL AGENCY shall have all powers allowed by law for interlocal agencies created under RCW 39.34.030 and Chapter 24.06 RCW, as authorized, amended, or removed by the Executive Board, as provided for in this Agreement and including but not limited to the following:

a. Recommend action to the legislative bodies of the Participating Cities;

b. Review and approve budget expenditures for the PORTAL AGENCY;

c. Establish policies for expenditures of budget items for the PORTAL AGENCY;

d. Review and adopt a personnel policy for the PORTAL AGENCY (if applicable);

e. Review and approve operating, Portal use, and financial policies for the PORTAL AGENCY;

f. Establish a fund or special fund or funds as authorized by RCW 39.34.030 for the operation of the PORTAL AGENCY;

g. Conduct regular and special meetings as may be designated by the Executive Board consistent with the state Open Public Meetings Act (Ch. 42.30 RCW) as now or hereafter amended;

h. Maintain and manage records in accordance with the state Public Records Act (Ch. 42.56 RCW) as now or hereafter amended, and other applicable state and federal laws and regulations;

i. Determine what services shall be offered and under what terms they shall be offered, consistent with Section 5.

j. Retain and terminate a Manager;

k. Create committees to review and make recommendations and carry out such functions and responsibilities as the Board may expressly provide;

l. Approve strategic plans;

m. Approve the addition of new Principals and new Subscribers and the terms of their participating in PORTAL AGENCY and receipt of PORTAL AGENCY services;

n. Enter into agreements with third parties for goods and services necessary to fully implement the purposes of this Agreement;

o. Establish fees and charges for services provided to Participating Cities or other parties, including but not limited to Taxpayers and Licensees using the services of the Portal;

p. Direct and supervise the activities of any committee established and/or any advisory boards, and the Manager;

q. Accept grants of funds from any federal, state, local or private agencies and receive and distribute such funds;

r. Receive all funds allocated to PORTAL AGENCY by Participating Cities;

s. Purchase, take, receive, lease, take by gift, or otherwise acquire, own, hold, improve, use and otherwise deal in and with real or personal property, or any interest therein, in the name of PORTAL AGENCY;

t. Sell, convey, lease, exchange, transfer, and otherwise dispose of all of its property and assets;

u. Sue and be sued, complain and defend, in all courts of competent jurisdiction in PORTAL AGENCY's name;

v. Make and alter bylaws for the administration and regulation of its affairs; and

w. Any and all other lawful acts necessary to further PORTAL AGENCY's goals and purposes.

x. Notwithstanding the foregoing, the PORTAL AGENCY shall not have the authority to issue debt in its own name.

The Portal Agency, as a joint instrumentality of its municipal corporation members under Chapter 39.34 RCW, shall have no powers or authority that are not held by Washington cities.

SECTION 7. EXECUTIVE BOARD: COMPOSITION AND OPERATION.

a. Composition. The Executive Board shall be composed of one (1) Board Member from each Principal, plus at least one (1) non-voting Board Member representing PORTAL AGENCY Subscribers. Such representatives are referred to as a Board Member or Board Members of the Executive Board.

b. Powers. The Executive Board shall have final decision-making authority upon all policy issues and shall exercise the powers described in Section 6**.** The Executive Board may delegate responsibility for execution of Executive Board policies and directives and for day-to-day operational decision-making to the Manager, including the hiring and supervision of additional staff positions authorized by the Executive Board, subject to the terms of Section 11.

c. Limitation on Total Number of Voting Board Members on Executive Board; Allocation of Executive Board Positions Among Multiple Principals. Notwithstanding the terms of Subsection 7.a, at no time shall the number of Executive Board Members exceed fifteen (15) voting members, and for so long as it remains a Principal, no Original Principal shall be required to share representation of its Board seat with another Principal. If the addition of a new Principal would cause the number of Executive Board voting Board Members to exceed fifteen (15), then the Principals with the smallest Population shall share a single Board Member position in order to reduce the number of Executive Board voting Board Members to fifteen (15); *provided that*, if over five (5) Principals would be represented by a single Board Member, then an additional

Board seat shall be converted for shared representation, to be shared by the Principals with the smallest Population. In the event that the number of Principals sharing representation is not evenly divisible by the number of shared seats, then the Principals with the larger Population shall be given the benefit of the allocation (e.g., if 7 Principals are to share 2 seats, then the 3 Principals with the largest Population (within the group sharing representation) shall share one (1) seat, and the four (4) Principals with the smallest populations shall share the second seat). If the number of Principals exceeds 59, then the same process as described above shall be repeated, that is, moving to a maximum of six (6) Principals sharing a seat, and so on (seven (7) Principals sharing a seat, etc.) as necessary to accommodate additional Principals.

d. Method of Determining Selection of Subscriber Representative(s) or Shared Voting Board Member(s). Subscribers shall initially share one (1) non-voting seat on the Executive Board. The Executive Board may by Supermajority Vote increase the number of non-voting seats for Subscribers and may define how such additional seats are allocated among Subscribers. Unless otherwise described in the Bylaws, Subscribers sharing representation of the non-voting Board Member shall determine the means by which to select their Executive Board representative and shall inform the Board of their choice at the time of the biennial Executive Board Officer elections (or at such other times as may be required in the event of a vacancy). Similarly, those Principals sharing representation on a single Executive Board seat shall determine the means by which to select the position, and shall make the determination at the same time as the biennial Executive Board Officer elections (or at such other times as may be required in the event of a vacancy).

i. Unless otherwise described in the Bylaws, in the event that Subscribers or Principals are unable to agree on a shared representative or Board Member on a timely basis, the remaining Executive Board Members may make the selection for them by a vote of the Executive Board.

ii. Individuals representing multiple Subscribers or Principals are expected to confer with the Cities they represent.

e. Qualifications to Serve on Executive Board. To serve on the Executive Board, as either a voting or non-voting Board Member, a person must be the appointing city's Chief Financial Officer (e.g., finance director or city treasurer, or equivalent), or their deputy or equivalent. An individual representing multiple cities on a single Executive Board seat or serving as the non-voting Subscriber representative shall similarly hold such a position within one of the Subscriber cities sharing such representation.

f. No Compensation for Serving on Executive Board. All Executive Board Members and their alternates shall serve without compensation from the PORTAL AGENCY. However, the PORTAL AGENCY may pay for or reimburse Executive Board Members and alternates for out-of-pocket costs related to service on the Executive Board.

g. Term of Office; Vacancies**.** Executive Board Members shall serve on the Executive Board for so long as they hold a position that qualifies them for the seat unless the city they represent elects to appoint another individual. Executive Board Members representing multiple Cities (either as a Principal or Subscriber) shall serve until the next Board Officer elections. Any vacancies shall be promptly filled by the appointing Principal, group of Principals, Subscribers, or the Executive Board (per Section 7.d.i), as appropriate.

h. Alternates. Each Executive Board Member shall have a single alternate designated in writing. Alternates must meet the same qualification as the designated Board Member or have similar financial expertise and be in a management position within their city.

i. Quorum. A simple majority of the Board Members (or their alternates) in number (excluding any Board Member which per Section 17 has given notice of withdrawal or which has been terminated by vote of the Executive Board) shall constitute a quorum of the Executive Board for purposes of taking action.

j. Voting. The Executive Board shall strive to operate by consensus. All Executive Board decision on items not listed in Section 7.k shall require a Simple Majority Vote for approval. A Board Member may not split his or her vote on an issue. No voting by proxies or mail-in ballots will be allowed. Voting by a designated Alternate is not considered a vote by proxy. A Board Member representing a Principal that has given notice of withdrawal or which has been terminated by vote of the Executive Board shall be authorized to cast votes at the Executive Board only on budget items to be implemented prior to the withdrawal or termination date.

k. Items Requiring a Supermajority Vote for Approval:

i. Approval or amendment of the budget or draft budget. (Per Section 13.b.iv, approval of the draft and final budget or amendments thereto also requires unanimous approval of the Original Principals in certain instances).

ii. Approval or amendment of user fees and charges.

iii. Approval of the Portal Operations Policy or amendments thereto.

iv. Adoption or amendment of the Bylaws or amendment of the Articles of Incorporation.

v. A decision to acquire assets, equipment, real or personal property, or bind the PORTAL AGENCY to pay total or cumulative any contract amounts over $50,000, *provided that,* this threshold amount will be indexed on the fifth anniversary of the formation of the PORTAL AGENCY and every five (5) years thereafter by the CPI-U Seattle-Tacoma-Bremerton.

vi. Admission of a new Principal.

vii. Admission of a new Subscriber.

viii. The decision to create an additional non-voting seat for Subscribers on the Executive Board.

ix. Addition of any staff positions, or partial staff positions, to support PORTAL AGENCY operations. (Per Section 13.b.iv, approval of funding for increases in the number of staff positions also requires unanimous approval of the Original Principals in certain instances).

x. Appointing or removing the Manager.

xi. Merger, consolidation, sale of all or substantially all assets of the PORTAL AGENCY (See Section 16).

xii. Amendment of the Agreement (except for those amendments requiring approval of all legislative bodies of the Principals per Section 18).

xiii. Termination or dissolution of the PORTAL AGENCY (See Section 19).

xiv. Any other action actions requiring a sixty-six percent (66%) Supermajority vote under Chapter 24.06 RCW.

l. Officers. The Executive Board shall have four officers, a Chair, Vice-Chair, Secretary and Treasurer. It will be the function of the Chair to preside at the meetings of the Executive Board. The Vice-Chair shall assume this role in absence of the Chair. At the first meeting of the Executive Board following the effective date of this Agreement, the officers shall be elected, and shall serve in this capacity through April 1, 2016, whereupon a new Chair and Vice-Chair shall be elected by the Executive Board. Biennially thereafter, the Executive Board shall elect a new Chair and Vice-Chair for two (2) year terms commencing each April 1. In the event of a vacancy in the Chair position, the Vice-Chair shall assume the Chair for the balance of the term of the departed Chair. In the event of a vacancy in the Vice-Chair position, the Executive Board shall elect a new Vice-Chair to serve the balance of the term of the departed Vice-Chair. An officer elected to fill the unexpired term of his or her predecessor shall not be precluded from serving one or more full annual terms of office following the end of such unexpired term. Any officer appointed by the Executive Board may be removed by vote of the Executive Board, with or without cause, in which event the Executive Board shall promptly elect a new officer who shall serve until the next regular officers' board term begins. The Executive Board may appoint persons other than Board Members of the Executive Board to serve as Secretary and Treasurer of the PORTAL AGENCY. The duties of all officers shall be further described in the PORTAL AGENCY Bylaws.

m. Staffing. The Manager shall assign agency staff to support the Executive Board as he or she deems appropriate.

n. Meetings. The Executive Board shall meet as often as it deems necessary and not less than once a year, at a time and place designated by the Chair of the Executive Board or by a majority of its Board Members. Not less than fourteen (14) days advance notice of regular

meetings shall be given. Special meetings may be called by the Chair or any two (2) Board Members upon giving all other Board Members not less than ten (10) days prior notice. In an emergency, the Executive Board may dispense with written notice requirements for special meetings, but must, in good faith, implement best efforts to provide fair and reasonable notice to all Executive Board Members. Board Members (or alternates) may participate in meetings by telephone conference or equivalent means of voice communication. At all times, the Executive Board shall comply with Ch. 42.30 RCW (Open Public Meetings Act).

o. Articles of Incorporation and Bylaws. Unless otherwise provided in the Articles and Bylaws or by vote of the Executive Board, upon the request of any Board Member of the Executive Board, Robert's Revised Rules of Order shall govern any proceeding of the Executive Board.

p. Consultation with Operations Committee. It is the intent of this Agreement to seek the active participation and advice of Participating Cities in the determination of PORTAL AGENCY policies and management. To the extent practicable, all items to come before the Executive Board shall have been previously subject to the review, comment and recommendation of the Operations Committee and the Executive Board shall consider input from the Operations Committee in its deliberations.

q. Consultation with Businesses, Taxpayers and Participating Cities. Not less than once each year the Executive Board shall seek input from Taxpayers and Participating Cities for the purpose of securing feedback and information on the efficiency and effectiveness of the Portal and PORTAL AGENCY programs.

SECTION 8. CONVERSION OF STATUS OF PARTICIPATING CITIES; ADDITION OF NEW PRINCIPALS OR SUBSCRIBERS.

a. Loss of Principal Status. As described in Sections 13.d and 13.k hereof, a Principal shall be converted to Subscriber for failure to approve its share of the budget or for nonpayment or delinquency in payment of charges and fees. On the date of such conversion, said former Principal shall:

i. lose its representation on the Executive Board;
ii. lose its right to receive a share of the PORTAL AGENCY assets upon dissolution of the PORTAL AGENCY;
iii. become subject to payment of charges and fees in accordance with the then applicable payment formula for Subscribers; and
iv. be bound by the terms of the then current Subscriber service contract.

The conversion of a Principal to Subscriber shall not discharge or relieve any Principal of its obligations to the PORTAL AGENCY or any other Participating City.

b. Election to Convert to Subscriber. A Principal may elect to convert to Subscriber status effective the first day of the next budget period by giving notice of its intent to the Governing Board not less than eight (8) months in advance of such effective date; *provided that*, a Principal may not exercise such election to take effect within the Initial Term. Such conversion shall be effective as proposed without further action of the Executive Board, barring any basis for terminating the Principal and action thereon by the Executive Board.

c. New Principals. A city or town otherwise meeting the qualifications of a Principal in Section 3.z hereof may be admitted to the PORTAL AGENCY as a Principal upon Supermajority Vote of the Executive Board as required under Section 7.k and its approval and execution of a document confirm. Similarly, a Subscriber may apply to the Executive Board to be converted to Principal status. As a condition of becoming a Principal, whether by conversion or new admission, the Executive Board may require payment or other contributions or actions by the new Principal as the Executive Board may deem appropriate consistent with the Bylaws and Portal Operations Policy, and may set such start date for service as it deems appropriate, it being the intention that the addition of new Principals shall not cause then-existing Principals to incur additional costs.

d. New Subscribers. The determination of whether to accept Subscribers shall be made by the Executive Board in a manner similar, and subject to such terms and conditions, as that for accepting new Principals, it being the intention that the addition of new Subscribers shall not cause then-existing Principals or Subscribers to incur additional costs.

SECTION 9. TAX AND FINANCE OPERATIONS COMMITTEE.

a. Role and Responsibilities. A Tax and Finance Operations Committee ("Operations Committee") shall be established to provide advice and recommendations to the Executive Board. The Executive Board may determine to direct the Operations Committee to perform specific responsibilities within Board-defined parameters. The Operations Committee shall endeavor to promote interagency collaboration, cooperation and information sharing between PORTAL AGENCY Principals and Subscribers. The Operations Committee shall:

i. Assist in the review and development of Portal Operations Policy and amendments thereto, Portal development options, proposed new service options, and such other matters as the Executive Board may direct;

ii. Make reports and recommendations to the Executive Board from time to time on matters the Operations Committee deems appropriate;

iii. Assist in the review and development of proposed PORTAL AGENCY budgets;

iv. Provide written recommendations with respect to the proposed budget to the Executive Board at the time the proposed budget is submitted to the Executive Board;

v. Provide advice, information and recommendations to the PORTAL AGENCY Manager and staff;

vi. Assist in communications to City Councils, legislators, business community on PORTAL AGENCY issues;

vii. Reach out to technology staff within their respective Cities for input and ideas, and to keep them apprised of PORTAL AGENCY issues;

viii. Brief their respective Executive Board Members in advance of Executive Board meetings.

b. Membership. Membership of the Operations Committee shall include one (1) Representative from each Principal, appointed by that Principal, plus at least one (1) representative, appointed by the Executive Board, to represent Subscribers. Each Principal shall also appoint in writing a designated alternate to serve on the Operations Committee in case of absence of the primary Representative**.**

c. Qualification to serve on Operations Committee. Representatives and their alternates shall be staff from the Principal they represent, with expertise in city tax policy and administration and/or city financial policy and administration. Persons serving on the Operations Committee are referred to as Representatives (or alternates) and shall serve without compensation from the PORTAL AGENCY.

d. Officers, Voting, Meeting Rules. The Operations Committee shall select a Chair and Vice-Chair from among the membership of the Operations Committee. Each Representative on the Committee shall have one vote. The meeting rules for the Operations Committee shall be further defined in the PORTAL AGENCY Bylaws.

e. Staffing. The Operations Committee shall be staffed by the Manager and such additional agency staffing as the Manager may deem appropriate.

SECTION 10. PORTAL AGENCY STAFFING.

a. The PORTAL AGENCY shall be staffed in such manner as the Executive Board determines, including but not limited to the use of loaned employees from Principals, consultants or other service providers, purchase of services from Principals or others, or hiring staff, or any combination of the foregoing.

b. As described in Section 13.b.iv.2 and Exhibit D, any increase in Labor Costs in excess of the New Participant Labor Cost Increment requires approval of a Supermajority Vote of the Executive Board as well as the approval of all Board Members representing all Original Principals.

SECTION 11. PORTAL AGENCY MANAGER.

a. Portal Agency Manager Appointment, Responsibilities and Authority. The Executive Board shall be responsible for the appointment and termination of a Manager of the PORTAL AGENCY, and shall request input from the Operations Committee, or any other standing committees created by the Executive Board, regarding any proposed appointment. The Manager shall:

i. Be responsible to the Executive Board and shall advise it from time to time on a proposed budget and other appropriate matters in order to fully implement the purposes of this Agreement;

ii. Administer the PORTAL AGENCY in its day-to-day operations consistent with the policies adopted by the Executive Board;

iii. Appoint persons to fill other staff positions, subject to confirmation by the Executive Board as the Board may require;

iv. Submit quarterly budget and operation performance reports to the Executive Board in a form acceptable to the Executive Board;

v. Undertake outreach to Taxpayers, Licensees and businesses, as well as to Participating Cities on the effectiveness of the PORTAL AGENCY operations and programs.

vi. Manage and oversee performance of the Vendor and other vendors or contractors providing services to the PORTAL AGENCY.

vii. Consult in advance with the Operations Committee on issues to come before the Executive Board, including but not limited to working with the Operations Committee in the development of the PORTAL AGENCY's budget and policies.

b. Qualifications, Retention and Termination. The Manager shall have experience in technical, financial and administrative fields and his or her appointment shall be on the basis of merit only. The Manager is an "at will" position and may be terminated from his or her position as Manager upon the Supermajority Vote of the Executive Board, without cause.

c. Legal Counsel, Accountants and Auditors. Only the Executive Board shall be authorized to hire or retain legal counsel and independent accountants and auditors. Other consultants may be designated in such manner as the Executive Board may determine subject to Sections 6 and 7.

d. Contracts and Support Services. Subject to the terms of the Bylaws, the Executive Board or the Manager with advice of the Operations Committee shall as necessary contract with appropriate local governments or other third parties for the use of space for its operations, and for staff and auxiliary services including, but not limited to, records, payroll, accounting, purchasing and data processing. Notwithstanding the foregoing, only the Executive Board may approve changes to the Portal Vendor(s) or Portal Vendor Services Contract.

SECTION 12. ASSIGNMENT OF PORTAL SERVICES CONTRACT FROM SEATTLE TO PORTAL AGENCY.

Promptly following the execution of this Agreement and the filing of such forms with the Washington Secretary of State as are necessary to incorporate the PORTAL AGENCY as a nonprofit corporation, The City of Seattle agrees to assign the Portal Services Contract to the PORTAL AGENCY, together with all rights and responsibilities appurtenant thereto and the PORTAL AGENCY shall agree to accept such assignment, rights and responsibilities, it being the intent of the parties to this Agreement that the PORTAL AGENCY shall assume all responsibility for overseeing and funding the work of the Vendor pursuant to such Portal Services Contract as soon as practicable following formation of the PORTAL AGENCY.

SECTION 13. BUDGET; COST ALLOCATION; CAPITAL COST RECOVERY CHARGES; PAYMENT OF CHARGES; DELINQUENCIES; RESERVE FUNDS.

a. Budget Fiscal Year. The budget fiscal year shall be either the calendar year, or two calendar years as the Executive Board may determine. The "budget period" corresponds to the fiscal year or years so determined by the Board.

b. Budget Approval. The Manager shall develop the proposed operating budget in consultation with the Operations Committee. The Manager and Executive Board shall use their best efforts to meet the budget schedule set forth below, but failure to meet a specified budget deadline shall not constitute a breach of this Agreement.

i. The Manager shall present a proposed budget to the Executive Board by no later than **May 1** prior to the commencement of the budget period, together with the Operation Committee's recommendations with respect to the proposed budget.

ii. By no later than **June 15**, the Executive Board shall (1) review and revise the draft budget as it deems appropriate; (2) approve the draft budget (including proposed charges to Participating Cities and any user fees to

Taxpayers and Licensees) by Supermajority Vote; and (3) forward same to Principals. The approved draft budget, and all proposed fees and charges shall be forwarded to Subscribers no later than **July 1**.

iii. The final budget shall be adopted by vote of the Executive Board effective no later than **December 31** prior to commencement of the budget period, after receiving information as to:

1. which Subscribers will be continuing to contract with the PORTAL AGENCY; and

2. which Principals have or will approve their shares of the PORTAL AGENCY budget, based on action or information from such Principals received by the PORTAL AGENCY no later than **December 1**.

iv. Vote Required to Approve Budget. Per Section 7.k.i, a Supermajority Vote of the Executive Board is required to approve the draft and final budget, *provided* that unanimous approval of the Executive Board Members representing all Original Principals shall also be required to approve any budget or budget amendment that includes:

1. An increase in Capped Costs greater than the maximum amount allowed per calculation of the New Participant Capped Cost Increment, as further described in Exhibit D.

2. An increase in Labor Costs to increase the number of full or partial staff positions greater than the maximum amount allowed per calculation of the New Participant Labor Cost Increment, as further described in Exhibit D.

v. 2014 Budget. Notwithstanding the foregoing, the PORTAL AGENCY budget for the year 2014 will be formally adopted by action of the Executive Board promptly following incorporation of the PORTAL AGENCY and need not be submitted for approval by the Original Principals. The proposed 2014 budget is set forth at Exhibit A. By approving this Agreement each Original Principal also approves their contribution to the 2014 budget in an amount not to exceed that shown in Exhibit A, promptly following the date the PORTAL AGENCY is incorporated.

c. Payment of Charges. The Board shall determine the timing of payments by Participating Cities, which shall be set forth in the Portal Operations Policy.

d. Failure of a Principal to Approve Budget Share. Failure of a Principal to approve its share of the budget before the commencement of the budget period shall result in the Principal being converted to Subscriber status effective as of the first day of the budget period for which the budget was not approved.

e. Notification of Final Adopted Budget. Promptly following final adoption of the budget by the Executive Board, the Manager shall provide notice to all Principals and Subscribers as to the terms of the final adopted budget, including their share of PORTAL AGENCY costs, charges and fees, and the payment schedule.

f. Budget Modifications. Modifications to the budget shall be approved by a Supermajority Vote of the Executive Board (and also unanimous consent of the Original Principals if required by Section 13.b.iv above) as necessary from time to time to account for changes in expenditures and revenues.

g. Cost Allocation and Cost Recovery Principles. The PORTAL AGENCY budget shall be generally allocated between all Participating Cities based on the number of Transactions processed for each City on the Portal. In years 2014 through 2018, the number of Transactions for the Original Principals shall be based on 2012 historical actual pre-Portal use Transaction Counts (set forth in Exhibit A) and the City Transaction Count for any other Participating City shall be based on the most recent historical data for that City prior to it joining the Portal. From and after 2019, the number of Transactions allocated to Original Principals shall be based on the most recent actual annual number of Transactions processed on the Portal for each such City (thus for 2019, the 2017 actual Transaction count will be used); for other Participating Cities, the allocation will be determined considering the actual number of Transactions (if the City had joined before 2019), historical tax and license information, and the experience of Original Principals as to how quickly businesses have adopted use of the Portal since its launch. The details of the cost allocation calculation shall be set forth in the Portal Operations Policy. Nothing in this Agreement shall be construed to prohibit the Executive Board from including factors in addition to the number of City Transactions in the cost allocation formulas as between Participating Cities, so long as the primary basis for allocation remains the City Transaction count.

h. User Fees. The PORTAL AGENCY shall impose such reasonable user fees as the Executive Board may determine on Taxpayers and Licensees utilizing the Portal to file tax returns or file business license applications in order to recoup costs of PORTAL AGENCY

operations, the Portal operation and maintenance, reserves and any other PORTAL AGENCY costs.

i. Estimated Six Year Operating Costs**.** Exhibit B sets forth a general estimate of the annual costs to establish and operate the PORTAL AGENCY between 2014 and 2020, assuming the Original Principals are the only Participating Cities, and includes estimated payment of Vendor's charges pursuant to the Portal Services Contract and other estimated operating costs. This Exhibit is an estimate and is not binding on any of the parties to this Agreement, nor is it binding on the PORTAL AGENCY.

j. Capital Cost Recovery Charge. In order to reimburse the City of Seattle for approximately one third of the costs Seattle paid to fund start-up of the Portal Agency, each Participating City other than the City of Seattle will be charged an annual Capital Cost Recovery Charge, in an amount described in Exhibit C. Such Charges shall be imposed each year from and after 2015 until such time as the total Capital Cost Recovery Charges paid reaches $1,400,000. The Capital Cost Recovery Charges will be paid by Participating Cities to the Portal Agency and the Portal Agency shall thereafter remit the total annual amount to Seattle. The Capital Cost Recovery Charge is not considered part of the Portal Agency budget for purposes of calculating Capped Costs or CPI-U limitations on the growth of such costs.

k. Payment and Delinquencies. Principals shall promptly pay fees and charges allocable to them. Interest on fees and charges allocable to any Principal not paid when due shall begin accruing interest immediately at the Federal Reserve Prime Rate as of the date the payment was originally due, plus 3% per year. The PORTAL AGENCY shall, within seven (7) days of the due date, send notice to any delinquent Principal and provide a 60-day cure period from the original due date of the payment. If such fees and interest penalties are not paid in full within 60 days of the original due date, then the Principal delinquent in payment of fees shall upon such 60th day be deemed immediately converted to the status of a Subscriber and subject to penalty as described in Section 8. In the event a Principal converted to Subscriber status by non-payment of fees shall not have paid in full all fees and interest owing by six (6) months after the original due date, then the Executive Board may terminate provision of the PORTAL AGENCY'S services to that former Principal. After one (1) year, the nonpaying former Principal shall be deemed to have withdrawn from this Agreement, but the termination of services shall not absolve the former Principal of its obligation to pay all fees and charges past due, together with interest.

l. Terms of Subscriber Contracts. Subscriber contracts shall include terms consistent with these delinquency provisions, that is, interest shall accrue on delinquent payments at the same rate as provided herein, and service may be terminated if fees and interest are not paid in full within six months.

m. Reserve Funds. The Executive Board may establish and fund reserve funds to support operations or capital investments for the PORTAL AGENCY, at levels the Executive Board determines to be appropriate; *provided* that general reserve funds may only be used to support general PORTAL AGENCY operations, maintenance and capital costs and may not be used in support of developing projects or services that will not be utilized by all Principals; and *provided further*, that no Principal shall be required to contribute to special reserves established exclusively in support of projects or services that the Principal has certified it does not intend to utilize or make available to its Taxpayers and Licensees.

n. Use of Funds. Consistent with any use imposed on particular funds by statute, ordinance, contract, this Interlocal Agreement or any bylaws adopted by PORTAL AGENCY, the PORTAL AGENCY may use any available funds for any purpose authorized by this Agreement in connection with an authorized project.

SECTION 14. RETAINED AUTHORITY AND RESPONSIBILITY OF PARTICIPATING AGENCIES.

Each Participating City shall retain the responsibility and authority for its operational departments and for such equipment and services as are required at its place of operation to connect to PORTAL AGENCY operations, including but not limited to each Participating City's computer and data systems managing processes that provide services the Portal delivers (the City's system of record). Each Participating City shall also retain the responsibility and authority for managing and maintaining the security and privacy of all data that the Participating City links to the Portal. Inter-connecting equipment and services will not be included in PORTAL AGENCY'S budget and operational program, except as the Executive Board may determine.

SECTION 15. OWNERSHIP OF PROPERTY.

a. Ownership of Property. Excepting the Portal which is owned by the Vendor, all property both real and personal, as well as intellectual property rights or licenses purchased or otherwise acquired pursuant to or in connection with this Agreement shall be owned or held in the name of the PORTAL AGENCY; provided, however, that the Executive Board may convey ownership of specific property, property or use rights.

b. Loaned Property. If any Participating City provides equipment or furnishings for PORTAL AGENCY'S use, title to the same shall rest with the respective local entity unless that equipment or furnishing is acquired by the PORTAL AGENCY.

c. Data. Each Participating City shall retain ownership of its own data and property that may be used in connection with Portal or PORTAL AGENCY operations.

SECTION 16. MERGER OR CONSOLIDATION, OR SALE OF ALL OR SUBSTANTIALLY ALL ASSETS.

Approval of the merger or consolidation of PORTAL AGENCY with another entity, or the sale of all or substantially all assets of PORTAL AGENCY, shall require a Supermajority Vote.

SECTION 17. WITHDRAWAL BY, OR TERMINATION OF, A PRINCIPAL.

a. Notice and Timing. Any Principal may withdraw its membership and terminate its participation in this Agreement by providing written notice to the Executive Board on or before December 31 in any year, and the Executive Board shall promptly inform all other Principals of such notice. That withdrawal shall become effective on the last day of the next calendar year. Notwithstanding the foregoing, no Principal may terminate its participation in this Agreement effective prior to the end of the Initial Term.

b. Obligations of departing Principal. A Principal who withdraws, is terminated, changes or is changed to Subscriber status ("departing Principal") shall hold the remaining Principals and Subscribers harmless against any resultant increased capital and/or operating costs allocated to them for the following two (2) budget years (plus the remainder of the current budget year, if applicable), with respect to any Executive Board approved project (excluding the initial launch of the Portal) in which the departing Principal is participating or has agreed to participate prior to notice of withdrawal or notice of change to Subscriber status, but such obligation shall exclude the cost of any Capital Cost Recovery Charges. Such obligation shall be reduced to the extent new Principals or Subscribers are allocated these costs that would otherwise have been chargeable to the departing Principal. After recouping such costs, the Executive Board may authorize reimbursement to the remaining Principals and Subscribers based on a depreciated value of the withdrawing or converting Principal's contribution.

c. Rights of departing Principal. Departing Principals shall have rights to copies of all data held by the PORTAL AGENCY relating to that Principal's Taxpayers and Licensee and other data relating specifically to the Principal.

d. The termination and/or withdrawal of a Principal shall not discharge or relieve any Principal of its obligations to the PORTAL AGENCY or other Participating Cities.

SECTION 18. AMENDMENT OF AGREEMENT.

This Agreement may be amended upon approval of a Supermajority Vote of the Executive Board except that any amendment affecting the following shall require consent of the legislative authorities of all Principals:

a. Expansion of the scope of services provided by the PORTAL AGENCY beyond the scope of expansion authorized in Section 5.c.
b. The terms and conditions of membership on the Executive Board.
c. Voting rights of Executive Board Members.
d. Powers of the Executive Board.
e. Principal contribution responsibilities.
f. Hold harmless and indemnification requirements.
g. Provisions regarding duration, termination or withdrawal.
h. The conditions of this Section.

This section shall not be construed to require legislative authority consent for the addition of a new Principal or agreement to serve an additional Subscriber, or to expand or contract the services purchased by any Principal or Subscriber or offered by the PORTAL AGENCY.

SECTION 19. TERMINATION OF AGREEMENT; DISSOLUTION OF AGENCY.

a. Generally. This Agreement may be terminated upon the approval of a Supermajority Vote of the Executive Board. The termination shall be by direction of the Executive Board to wind up business by a date specified by the Executive Board, which date shall be at least one (1) year following the date of the vote to terminate. Upon the final termination date, this Agreement shall be fully terminated.

b. Distribution of Property on Termination of Agreement. Upon termination of this Agreement, all property acquired during the life of the Agreement remaining in ownership of PORTAL AGENCY shall be disposed of in the following manner:

i. Real or Personal Property. All real or personal property purchased pursuant to this Agreement and all unexpended funds or reserve funds, net of all outstanding PORTAL AGENCY liabilities, shall be distributed to those Principals still participating in the PORTAL AGENCY on the day prior to the termination date and shall be apportioned between Principals based on the ratio that the average of each Principals' contributions to the operating budget over the preceding five (5) years bears to the total of all then remaining Principals' user fees paid during such five-year period. The Executive Board shall have the discretion to allocate the real or personal

property and funds as it deems appropriate, and the apportionment, determined consistent with the preceding sentence, need not be exact.

ii. Intellectual Property Rights. The Vendor will own, or have rights to, all its intellectual property per the terms of the Portal Services Contract, including the right to license the Portal operating system exclusively to the PORTAL AGENCY, its Principals and Subscribers. The Portal license rights, and all rights granted relating thereto, terminate with the termination of the Portal Services Contract. Notwithstanding this termination, the Principals and Subscribers shall retain the right after termination of the Portal license rights to acquire any and all information and data, including but not limited to Taxpayer, Licensee and their respective City data, then currently held by the Vendor or the PORTAL AGENCY. Upon termination of the Portal Development and Services Contract or the dissolution of the PORTAL AGENCY, any and all intellectual property owned by the PORTAL AGENCY (which excludes the Portal and any other intellectual property owned by the Vendor) will be transferred in its entirety to Principal with the largest Population. If said Principal does not agree to accept the intellectual property owned by the PORTAL AGENCY, it shall then be transferred in its entirety to the Principal with the next largest population, and so on should that Principal not agree to accept the intellectual property. If no Principal agrees to accept the intellectual property, then the Executive Board will attempt to sell the intellectual property at fair market value and distribute the proceeds in proper proportion to the current Principals in accordance with Subsection 19.b.i.

iii. Loaned Property. In the event of dissolution or termination of the PORTAL AGENCY, assigned or loaned assets shall be returned to the lending entity.

iv. Allocation of Liabilities. In the event outstanding liabilities of the PORTAL AGENCY exceed the value of personal and real property and funds on hand, all Principals shall contribute to retirement of those liabilities in the same manner as which they would share in the distribution of properties and funds.

c. the foregoing, the Agreement may not be terminated if to do so would abrogate or otherwise impair any outstanding obligations of the PORTAL AGENCY, unless provision is made for those obligations.

SECTION 20. DISPUTE RESOLUTION.

a. Whenever any dispute arises between a Principal or the Principals or between the Principals and the PORTAL AGENCY (referred to collectively in this section as the "parties")

under this Agreement, which is not resolved by routine meetings or communications, the parties agree to seek resolution of such dispute by the process described in this section, which shall also be binding on Subscribers**.**

b. The parties shall seek in good faith to resolve any such dispute or concern by meeting, as soon as feasible. The meeting shall include the Chair of the Executive Board, the Manager, and a representative(s) of the Principal(s), if a Principal(s) is involved in the dispute, and/or a person designated by the Subscriber(s), if a Subscriber(s) is involved in the dispute.

c. If the parties do not come to an agreement on the dispute or concern, any party may request mediation through a process to be mutually agreed to in good faith between the parties within 30 days, which may include binding or nonbinding decisions or recommendations (whichever is mutually agreed to). The mediator(s) shall be mutually agreed upon and shall be skilled in the legal and business aspects of the subject matter of this Agreement. The parties shall share equally the costs of mediation and assume their own costs.

SECTION 21. INSURANCE.

The Executive Board, Manager, and Operations Board shall take such steps as are reasonably practicable to minimize the liability of the Participating Cities, including but not limited to the utilization of sound business practice. The Executive Board shall determine which, if any, insurance policies may be reasonably practicably acquired to cover the operations of the Portal Agency and the activities of the Parties pursuant to this Agreement (which may include Directors and Officers, Commercial General Liability, Auto, Workers' Compensation, Stop Gap/Employer's Liability, errors and omissions, crime/ fidelity insurance, CyberRisk), and shall direct the acquisition of same. [

SECTION 22. INDEMNIFICATION AND HOLD HARMLESS.

Each Principal shall indemnify and hold other Principals, their officers, officials, employees, agents and volunteers harmless from any and all claims, injuries, damages, losses or suits including attorney fees, arising out of that Principal's negligent acts or omissions in connection with the performance of its obligations under this Agreement, except to the extent the injuries or damages are caused by another Principal.

a. Each Principal shall indemnify and hold the PORTAL AGENCY and its officers, officials, employees and volunteers harmless from any and all claims, injuries, damages, losses or suits including attorney fees, arising out of that Principal's negligent acts or omissions in connection with the performance of its obligations under this Agreement, except to the extent the injuries and damages are caused by the PORTAL AGENCY.

b. As provided in its Articles of Incorporation, the PORTAL AGENCY shall indemnify and hold each Principal its officers, officials, employees and volunteers harmless from any and all claims, injuries, damages, losses or suits including attorney fees, arising out of the PORTAL AGENCY'S acts or omissions in connection with the performance of its obligations under this Agreement, except to the extent the injuries and damages are caused by any Principal.

c. Subscribers shall be required to agree to indemnify and hold harmless each Principal and the Portal Agency, their officers, officials, employees and volunteers from any and all claims, injuries, damages, losses or suits including attorney fees, arising out of Subscribers negligent acts or omissions in connection with its use of the Portal. To such degree as the Executive Board determines to be reasonable, appropriate, and consistent with applicable law and to be in the best interests of the Portal Agency, the Portal Agency may also indemnify and hold harmless Subscribers.

d. Should a court of competent jurisdiction determine that this Agreement is subject to RCW 4.24.115, then, in the event of liability for damages arising out of bodily injury to persons or damages to property caused by or resulting from the concurrent negligence of a party hereto and the PORTAL AGENCY, its officers, officials, employees, and volunteers, the party's liability hereunder shall be only to the extent of the party's negligence. It is further specifically and expressly understood that the indemnification provided in this Section constitutes the party's waiver of immunity under Industrial Insurance Title 51 RCW, solely for the purpose of this indemnification. This waiver has been mutually negotiated by the parties. The provisions of this section shall survive the expiration or termination of this Agreement.

e. Each party shall give the other parties proper notice as provided in Section 24, of any claim or suit coming within the purview of these indemnities. Termination of this Agreement, a Principal's withdrawal from the PORTAL AGENCY, or a Principal's conversion to Subscriber status (collectively for purposes of this subparagraph "Termination"), shall not affect the continuing obligations of each of the parties as indemnitors hereunder with respect to those indemnities and which shall have occurred prior to such Termination.

SECTION 23. INTERGOVERNMENTAL COOPERATION.

The PORTAL AGENCY shall cooperate with local, state and federal governmental agencies in order to maximize the utilization of any grant funds for equipment and operations and to enhance the effectiveness of the PORTAL AGENCY's operations and minimize costs of service delivery.

SECTION 24. NOTICE.

Notices required to be given to the PORTAL AGENCY under the terms of this Agreement shall be directed to the following unless all Principals are otherwise notified in writing:

Chair, PORTAL AGENCY Executive Board
c/o his/her Principal agency's address

Notices to Principals or Subscribers, Board Members or Representatives required hereunder may be given by mail, overnight delivery, facsimile or email (with confirmation of transmission), telegram, or personal delivery. Each Principal shall provide the Chair of the PORTAL AGENCY Executive Board written notice of the address for providing notice to said Principal. Any Principal wishing to change its mail or email address shall promptly notify the Chair of the Executive Board. Notice or other written communication shall be deemed to be delivered at the time when the same is postmarked in the mail or overnight delivery services, sent by facsimile or email (with confirmation of transmission), sent by telegram, or received by personal delivery.

SECTION 25. VENUE.

The venue for any action related to this Agreement shall be in the Superior Court in and for King County, Washington at Seattle, or if applicable, in Federal District Court, Western District of Washington.

SECTION 26. FILING.

As provided by RCW 39.34.040, this Agreement shall be filed prior to its entry in force with the King County Department of Executive Services Division of Records and Licensing Services, or its successor, Records and Elections, or, alternatively, listed by subject on a Principal's web site or other electronically retrievable public source.

SECTION 27. NO THIRD-PARTY BENEFICIARIES.

There are no third-party beneficiaries to this Agreement. No person or entity other than a party to this Agreement shall have any rights hereunder or any authority to enforce its provisions, and any such rights or enforcement must be consistent with and subject to the terms of this Agreement.

SECTION 28. SEVERABILITY.

The invalidity or any clause, sentence, paragraph, subdivision, section or portion of this agreement shall not affect the validity of the remainder of the Agreement.

SECTION 29. RATIFICATION.
All prior acts taken by the Principals and the PORTAL AGENCY consistent with this Agreement are hereby ratified and confirmed.

SECTION 30. EXECUTION, COUNTERPARTS AND EFFECTIVE DATE.

This Agreement and any amendments thereto, shall be executed on behalf of each Principal by its duly authorized representative and pursuant to an appropriate motion, resolution or ordinance. This Agreement may be executed in any number of counterparts, each of which shall be an original, but those counterparts will constitute one and the same instrument. This Agreement shall be deemed adopted and effective as of March 1, 2014, subject to prior approval by the legislative bodies of all four Original Principals, execution by each Original Principal, and prior filing of same as required by Section 26.

//
//
(Remainder of page left blank intentionally)
//
//
//
//

IN WITNESS WHEREOF, this Agreement has been executed by each party on the dates set forth below.

City of Bellevue

_____
City Manager

_____
Date
Approved as to Form:

_____
City Attorney

_____
Date

City of Everett

_____
Mayor

_____
Date
Approved as to Form:

_____
City Attorney

_____
Date

The City of Seattle

_____
Mayor

_____
Date

Approved as to Form:

_____
City Attorney

_____
Date

City of Tacoma

_____
City Manager

_____
Date

Approved as to Form:

_____
City Attorney

_____
Date

IN WITNESS WHEREOF, this Agreement has been executed by each pa1iy on the dates set fo1i h below.

City of Bellevue

City Manager
1-31-14
Date
Approved as to Form:

Date

City of Everett

Mayor

Date
Approved as to Form:

City Attorney

Date

The City of Seattle

Mayor

Date

Approved as to Form:

City Attorney

Date

City of Tacoma

City Manager

Date

Approved as to Form:

City Attorney

Date

IN WITNESS WHEREOF, this Agreement has been executed by each party on the dates set forth below.

City of Bellevue

City Manager

Date

Approved as to Form:

City Attorney

Date

City of Everett

Ray Stephanson

Mayor

1-29-2014

Date

attest: Sharon Fuller
City Clerk

Approved as to Form:

City Attorney

1/27/14

Date

The City of Seattle

Mayor

Date

Approved as to Form:

City Attorney

Date

City of Tacoma

City Manager

Date

Approved as to Form:

City Attorney

Date

IN WITNESS WHEREOF, this Agreement has been executed by each party on the dates set forth below.

City of Bellevue

City Manager

Date

Approved as to Form:

City Attorney

Date

City of Everett

Mayor

Date

Approved as to Form:

City Attorney

Date

The City of Seattle

Mayor

Date

Approved as to Form:

of, City Attorney

Date

City of Tacoma

City Manager

Date

Approved as to Form:

City Attorney

Date

IN WITNESS WHEREOF, this Agreement has been executed by each party on the dates set forth below.

City of Bellevue

City Manager

Date
Approved as to Form:

City Attorney

Date

The City of Seattle

Mayor

Date

Approved as to Form:

City Attorney

Date

City of Everett

Mayor

Date
Approved as to Fonn:

City Attorney

Date

City of Tacoma

City Manager
12/19/2013
Date

Approved as to Form:

Debra Casper Deputy

l.:J,- 13-/3
Dat

12-18-2013
Andy Cherullo Date
Director of Finance

Attest:

.....
}-30 13
Doris Sorum Date
City Clerk

ORIGINAL

List of Exhibits

A. Proposed 2014 PORTAL AGENCY BUDGET SUMMARY (including number of Transactions used for cost allocation as between Original Principals)

B. 2015-2020 Estimated PORTAL AGENCY Operating Budget Summary

C. Capital Cost Recovery Charges

D. Calculation of New Participant Capped Cost Increment and New Participant Labor Cost Increment

Exhibit A

Proposed 2014 PORTAL AGENCY OPERATING BUDGET SUMMARY (including number of Transactions used for cost allocation as between Original Principals)

(June to December 2014)

Labor Total[1]	152,649
Contracts Total[2]	27,000
Overhead Total[3]	12,500
Vendor Costs[4]	180,208
Operating Reserves	55,854
Total Budgeted Costs	**428,210**
Total Budgeted Revenues	**428,210**
Estimated User fee Revenues[5]	72,566
Estimated Revenue from City Cost Allocations[6]	355,644
City of Seattle Cost Allocation[7]	*245,394*
City of Bellevue Cost Allocation	*35,654*
City of Tacoma Cost Allocation	*56,903*
City of Everett Cost Allocation	*17,782*

This budget estimates a six-month budget beginning after the Multi-City Business License and Tax Portal is up and running in mid-2014, the first six months are covered by the Portal

[1] This budget includes 2.5 FTE: the Portal Manager, a half-time administrative assistant and a full-time IT Project Manager/Business Analyst. The personnel for these positions will be provided by the City of Seattle and the costs in this budget include the fully-funded (salary, benefits, etc.) labor costs for all 2.5 positions. A separate loaned staffing agreement will be entered into between the Portal Agency and the City of Seattle in 2014 for these staff.

[2] Includes contracts for outside services such as Accounting, Insurance, Bank and the State Auditor.

[3] Funding for miscellaneous overhead items such as legal fees, office and operating supplies, printing and licenses/memberships.

[4] Includes costs estimated payable to-Gov Systems under the Portal Services Contract in 2014, from and after the Portal goes "live." For the first five years of Portal operation e-Gov Systems will charge the Portal Agency $1.25 every time a business or taxpayer makes an online Portal filing, whether or not tax is owing.

[5] Assumes the Executive Board approves a proposed user fee of $4 per online session per City (the proposed fee would be payable only when tax is owed; multiple tax and/or license filings on the same session would incur only one fee). This user fee is based on an estimated Portal use adoption rate by business and taxpayers of 15%. This adoption rate is expected to grow considerably each year.

[6] Cost Allocations are based on the 2012 Transaction count for each Original Principal, shown in the table at the End of this Exhibit A.

[7] Excludes Seattle's contributions to start-up costs in 2014. Also excludes labor and operating costs for which Seattle will be reimbursed from the Total Budget shown above, per the loaned staffing agreement.

Implementation Project costs funded by Seattle. This budget estimates also assumes only four cities participate in 2014.

Transaction Counts Calculations used for Cost Allocation as between Original Principals

Transaction Counts	Based on 2012 actual business license filings, business and occupations and gross receipts tax filings for each Original Principal				
	Seattle	**Bellevue**	**Tacoma**	**Everes t t**	**Total**
Transactions	212,457	30,927	50,000	14,392	307,776
% Allocation	69%	10%	16%	5%	100%

Exhibit B:

Multi-City Business License and Tax Portal Agency
2015-2020 Estimated Operating Budget Summary

This budget is an estimated six-year budget and assumes only four cities participating.

	2015	2016	2017	2018	2019	2020
Labor Total[8]	314,740	324,182	333,908	343,925	354,243	364,870
Contracts Total[9]	55,188	56,402	57,643	58,911	60,207	61,532
Overhead Total[10]	15,330	15,667	16,012	16,364	16,724	17,092
Vendor Total[11]	344,888	383,360	421,832	460,304	479,540	498,776
Operating Reserve - 15%	53,668	7,420	7,467	7,516	4,681	4,733
Total Estimated Budget	783,814	787,031	836,862	887,021	915,396	947,003
Estimated User Fee Revenue[12]	193,510	241,888	290,266	338,643	362,832	387,021
Estimated City Cost Allocation Revenues[13]	602,057	555,622	557,306	559,322	563,749	571,414
City of Seattle[14]	415,419	383,379	384,541	385,932	388,987	394,276
City of Bellevue	60,206	55,562	55,731	55,932	56,375	57,141
City of Tacoma	96,329	88,900	89,169	89,492	90,200	91,426
City of Everett	30,103	27,781	27,865	27,966	28,187	28,571

[8] This budget includes 2.5 FTE: the Portal Manager, a half-time administrative assistant and a full-time IT Project Manager/Business Analyst. The personnel for these positions will be provided by the City of Seattle and the costs in this budget include the fully-funded (salary, benefits, etc.) labor costs for all 2.5 positions. A separate loaned staffing agreement will be entered into between the Portal Agency and the City of Seattle in 2014 for these staff.
[9] Includes contracts for outside services such as Accounting, Insurance, Bank and the State Auditor.
[10] Funding for miscellaneous overhead items such as legal fees, office and operating supplies, printing and licenses/memberships.
[11] Includes costs estimated payable to-Gov Systems under the Portal Services Contract in 2014, from and after the Portal goes "live." e-Gov Systems will charge the Portal Agency $1.25 every time a business or taxpayer makes an online Portal filing, whether or not tax is owing. This per-filing cost is fixed for the first five years of Portal operation.
[12] Assumes the Executive Board approves a proposed user fee of $4 per online session per City (the proposed fee would be payable only when tax is owed; multiple tax and/or license filings on the same session would incur only one fee). This user fee is based on an estimated Portal use adoption rate by business and taxpayers of 15%. This adoption rate is expected to grow considerably each year.
[13] Cost Allocations are based on the 2012 Transaction count for each Original Principal, shown in Table 2.
[14] Excludes Seattle's contributions to start-up costs in 2014. Also excludes labor and operating costs for which Seattle will be reimbursed from the Total Budget shown above, per the loaned staffing agreement.

Transaction Counts Calculations used for Cost Allocation as between Original Principals

Transaction Counts	Based on 2012 actual business license filings, business and occupations and gross receipts tax filings for each Original Principal				
	Seattle	**Bellevue**	**Tacoma**	**Everet t**	**Total**
Transactions	212,457	30,927	50,000	14,392	307,776
% Allocation	69%	10%	16%	5%	100%

Estimated Adoption Rates

e-Gov Systems Recommended Adoption Rate	This is the recommended rate of adoption from e-Gov systems based on previous implementations.					
	2015	**2016**	**2017**	**2018**	**2019**	**2020**
Adoption Rate	40%	50%	60%	70%	75%	80%

CPI-U Rates Forecast

	2014	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**
CPI-U Forecast (Bellevue)	2.20%	2.20%	2.20%	2.30%	2.30%	2.30%	2.30%

Exhibit C

Capital Cost Recovery Charges

Beginning in 2015, every Participating City other than the City of Seattle will pay a yearly Capital Cost Recovery Charge to the Portal Agency which in turn will remit the annual total of such Charges paid to the City of Seattle. The Charges will remain in place until the total amount of $1,400,000 has been remitted to Seattle.

The Executive Board shall determine the timing for payment of the Capital Cost Recovery Charges.

Each Participating City's Capital Cost Recovery Charge will be determined based on the number of Transactions allocated to such City in the budget year in which the Charge will be collected, and in accordance with the following table:

Category:	**Smallest City**	**Smaller City**	**Small City**	**Medium City**	**Large City**
Transaction Count allocated to the City in the budget year	< 1000	1001 - 4000	4,001 to 14,400	14,401 to 31,000	>31,001
Capital Cost Recovery Charge payable annually	**$500**	**$1000**	**$2000**	**$4000**	**$6000**

Exhibit D

Calculation of New Participant Capped Cost Increment and New Participant Labor Cost Increment

New Participant Capped Cost Increment.

The New Participant Capped Cost Increment is an amount calculated in the development of each budget (or budget amendment) to identify the maximum amount by which Capped Costs may increase in the budget period *without requiring unanimous consent of the Executive Board Members representing all four Original Principals*. The Increment is determined by identifying the "CPI-U Limit for Capped Costs per Transaction" for the applicable budget period, assuming the Portal Agency has the same number of Participating Cities as the prior budget period and the Capped Costs from the previous period are inflated by the CPI-U Limit. The Capped Cost per Transaction is then multiplied by the number of Transactions attributable to new Participating Cities joining the Portal Agency in the budget period, and the resulting total is the maximum amount by which the Capped Costs in the new budget period may be increased over and above the Status Quo Capped Cost *without requiring unanimous consent*.

Illustration: **Calculation of New Member Capped Cost Increment for Year X** *Assuming: 1-year budget period; addition of 2 member cities proposed in Year X*	
Part 1: Calculating CPI-U Limit for Capped Costs Per Transaction	
CPI-U Limit for Capped Cost for Year X, • Inflate Capped Costs for the previous year by the CPI-U Limit.	$16,000
Estimated Transaction Count for Year X from currently Participating Cities • Includes all Cities participating as Principals or Subscribers in the previous year. • Transaction count is that used for purposes of estimating the cost allocations of these Participating Cities in Year X.	125,000
Capped Cost Per Transaction ($16,000 ÷ 125,000)	**$0.128**
Part 2: Calculating New Member Capped Cost Increment	
New Member Transaction Count • Total Transactions assigned to the 2 new Participating Cities for purposes of budget allocation in Year X	10,000
New Member Capped Cost Increment for Year X ($0.13 x 10,000)	**$1,280**
Capped Costs in Year X may be increased by Supermajority Vote to a level of $17,280. Capped Costs in excess of that amount would require Supermajority Vote and unanimous approval by Board Members representing the Original Principals.	

New Member Participant Labor Cost Increment.

The New Participant Labor Cost Increment is an amount calculated in the development of each budget (or budget amendment) to identify the maximum amount by which Labor Costs may increase in the budget period *without requiring unanimous consent of the Executive Board Members representing all four Original Principals.* The Increment is determined by identifying the "Status Quo Labor Cost per Transaction" for the applicable budget period, assuming the Portal Agency has the same number of Participating Cities and staff as the prior budget period. The Labor Cost per Transaction is then multiplied by the number of Transactions attributable to new Participating Cities joining the Portal Agency in the budget period, and the resulting total is the maximum amount by which the Labor Costs in the new budget period may be increased over and above the Status Quo Labor Cost *without requiring unanimous consent*.

Illustration: **Calculation of New Participant Labor Cost Increment for Year X** *Assuming: 1-year budget period; addition of 2 member cities proposed in Year X*	
Part 1: Labor Cost Per Transaction	
Status Quo Labor Costs for Year X • Assuming same number of staff (including employees, if any, and loaned staff) as were engaged by the Portal Agency in the previous year, and adding any estimated increases in costs of salary, benefits, etc. for those same personnel over and above the previous year's costs.	$350,000
Estimated Transaction Count for Year X from Currently Participating Cities • Includes all Cities participating as Principals or Subscribers in the previous year. • Transaction count is that used for purposes of estimating the cost allocations of these Participating Cities in Year X.	125,000
Labor Cost Per Transaction ($350,000 ÷ 125,000)	**$2.80**
Part 2: New Participant Labor Cost Increment	
New Participant Transaction Count • Total Transactions assigned to the 2 new Participating Cities for purposes of budget allocation in Year X	10,000
New Participant Labor Cost Increment for Year X ($2.80 x 10,000)	**$28,000**
*Labor Costs in Year X may be increased by Supermajority Vote to a level of $378,000. Labor Costs in excess of that amount would require Supermajority Vote **and** unanimous approval by Board Members representing the Original Principals.*	

BYLAWS

APPENDIX NO. A3

BYLAWS

OF

WASHINGTON MULTI-CITY BUSINESS LICENSE AND TAX PORTAL AGENCY

("PORTAL AGENCY")

ARTICLE I. PURPOSES

As set forth in the Washington Multi-City Business License and Tax Portal Agency Interlocal Agreement dated as of March 1, 2014, by and between the Cities of Bellevue, Everett, Seattle and Tacoma (the "Agreement"), the PORTAL AGENCY is organized in accordance with the Interlocal Cooperation Act (Chapter 39.34 RCW) and the Nonprofit Miscellaneous and Mutual Corporations Act (Chapter 24.06 RCW) as a public body and instrumentality of its members to jointly exercise essential governmental functions of its members.

ARTICLE II. DEFINITIONS; CONFLICTING PROVISIONS

All capitalized terms used and not otherwise defined in the Bylaws shall have the meaning set forth in the Agreement. In the event of a conflict between a provision of the Bylaws and a provision of the Agreement, the provision of the Agreement shall prevail.

ARTICLE III. OFFICES

The principal office and place of business of the PORTAL AGENCY in the state of Washington shall be initially located at Seattle City Hall, 600 4th Avenue, Seattle, WA 98104. The name and address of its initial registered agent is Glen Lee, Finance Director, City of Seattle, 700 Fifth Avenue, Suite 4350, Seattle, WA 98104.

ARTICLE IV. BOARD

Section 4.1. General Powers. The business and affairs of the PORTAL AGENCY shall be managed by its Executive Board (referred to in these Bylaws as either the "Executive Board" or "Board"), which shall be deemed a "Board of Directors" as that term is used in RCW 24.06.125. In addition to its other powers and authority set forth in the Agreement and subject to

applicable law, the terms of the Agreement or the terms of any gift, devise, bequest or other transfer, the Board shall have the full power, in its sole discretion, to change the form of any investment and, for that or other purpose of the PORTAL AGENCY, to dispose of any property held by the PORTAL AGENCY. The Board shall have the right to employ or retain persons or entities to carry out the purposes of the PORTAL AGENCY, including but not limited to attorneys, consultants, engineers, contractors and accountants.

Section 4.2 Composition of Board. The Board of the PORTAL AGENCY shall consist of one individual representative from each member entity ("Principal" as that term is defined in the Agreement), except as shared representation of Principals may be required by terms of Section 7.c of the Agreement. In addition, from and after such time as the PORTAL AGENCY has at least one Subscriber, there shall be one (1) non-voting Board Member representing Subscribers. Each representative is a "director" as that term is used in RCW 24.06.130, and is referred to in the Agreement as a "Board Member" and in these Bylaws as a "Board Member." Board Members representing a single Principal or Subscriber agency shall not have terms but rather each such Board Member shall serve at the pleasure of the agency that the Board Member represents. Board Members representing multiple Principals or Subscribers shall be elected biennially in accordance with Section 7.d of the Agreement. In order to serve as a Board Member, an individual must be the Chief Financial Officer (CFO) or deputy or equivalent of the represented agency (or the CFO, deputy or equivalent of one of the represented Principals or Subscribers, in the case of a Board Member representing multiple Principals or Subscribers).

Section 4.3 Designation and Qualifications of Alternates. Each member of the Executive Board shall designate in writing an alternate who shall serve as a member of the Executive Board during his or her absence or unavailability to serve, and in such case the alternate shall have the full rights and privileges of the absent member. Alternates must meet the same qualifications as the designated Board member or have similar financial expertise and be in a management position within their City. All written designations shall become effective upon delivery to the Chair of the Executive Board and shall remain in effect until revoked in writing by the designating member(s). In the event of any question of authority to act as an alternate, the determination of the Chair based upon the records on file with the Chair shall be determinative.

Section 4.4 Tenure. Unless the Board Member resigns or is removed in accordance with these Bylaws, each Board Member shall hold office until replaced by resolution or written motion of the legislative body of the appointing Principal. Notwithstanding the foregoing, no Board Member shall continue in that capacity if he or she no longer holds a position that qualifies him or her for the seat, and Board Members representing multiple Principals or

Subscribers shall be re-appointed every biennium consistent with the terms of Section 7.d of the Agreement.

Section 4.5 Annual and Regular Meetings. The annual meeting of the PORTAL AGENCY shall be held in March of each year, at such time and place as may be determined by the Executive Board, for the transaction of such business as may come before the meeting. The Executive Board may specify by resolution the time and place for holding any other regular Board meetings and notice for such meetings shall be given as required by the Agreement. Not less than fourteen (14) days advance notice shall be given of regular meetings.

Section 4.6 Special Meetings. Special meetings of the Board may be called by the Chair or by the written request of not less than two Executive Board Members, upon giving all other Board Members not less than ten (10) days prior notice. Notice of special meetings of the Board stating the date, time and place thereof shall be delivered to Board Members in accordance with RCW 24.06.104, as it may be amended and as otherwise required by the Agreement. The notice must be written or by electronic means. Notice shall also be given to any other persons as may be required by the Open Public Meetings Act (Chap. 42.30 RCW) and other applicable law. In an emergency, the Executive Board may dispense with written notice requirements for special meetings but must in good faith implement best efforts to provide fair and reasonable notice to all Executive Board meetings.

Section 4.7 Matters Requiring Notice. Prior written notice meeting the requirements of notice for special meetings shall be required in the case of action on any of the following matters:

A. All elections of the Chair or the recall of the Chair;
B. Budget approval and amendments;
C. Dues and assessments;
D. All final action on any commitment to an expenditure not authorized by an approved budget;
E. Contractual commitments requiring expenditures not previously authorized;
F. Changes in the Bylaws of PORTAL AGENCY;
G. Changes in membership; and
H. Reversal or modification of Executive Board decisions or modification of Executive Board authority or duties.

Section 4.8 Waiver of Notice of Special Meeting. Whenever any notice is required to be given to any Board Member pursuant to applicable law, a waiver in writing signed by the Board Member, entitled to notice, shall be deemed equivalent to the giving of notice. Any Board Member may waive notice of any meeting at any time. The attendance of a Board Member at a

meeting shall constitute a waiver of notice of the meeting except where a Board Member attends a meeting for the express purpose of objecting to the transaction of any business because the meeting is not lawfully convened. Unless otherwise required by law, neither the business to be transacted at, nor the purpose of, any regular or special meeting of the Board need to be specified in the notice or waiver of notice of such meeting.

Section 4.9 Quorum. A simple majority of the Members (or their alternates) in number (excluding any Member which per the Agreement has given notice of withdrawal or which has been terminated by voted of the Executive Board) shall constitute a quorum of the Executive Board for purposes of doing business at any time. Members may attend meetings by telephone conference or equivalent means of voice communication.

Section 4.10 Manner of Acting; Rules of Order. The Board shall strive to operate by consensus. All Board decisions on items not listed in Section 7.k of the Agreement or as otherwise specified in Sections 16, 18 and 19 of the Agreement, require a Simple Majority Vote for approval. A Member may not split her or her vote on an issue. No voting by proxies or mail-in ballots will be allowed. Unless otherwise approved by vote of the Executive Board, upon the request of any Member of the Executive Board, Robert's Revised Rules of Order shall govern any proceeding of the Executive Board. The Board may act by voice votes called for by the Chair, but any Member may require a recorded tabulation of votes by making a request either immediately before the vote is taken or immediately after a voice vote is taken.

Section 4.11 Supermajority Voting. Supermajority Voting shall be required on those items listed in Section 7.k of the Agreement. A "Supermajority Vote' means Executive Board approval of an item accomplished by securing affirmative votes of not less than sixty-six percent (66%) of all voting Board Members of the Executive Board in number, and not less than sixty-six percent (66%) in number of the Original Principals (the Cities of Bellevue, Everett, Seattle and Tacoma).

Section 4.12 Advisory and Board Committees. In addition to the Tax and Finance Operations Committee ("Operations Committee") established by the Agreement, and subject to the terms of the Agreement, the Executive Board may create other special advisory committees as it deems appropriate, and members of such advisory committees shall be appointed by the Executive Board. Persons who serve as members of any advisory committee are not be required to be Board Members or elected officials. The Board also may create standing or special committees of the Executive Board. Chairpersons and other members of standing committees or special committees (which excludes the Operations Committee) shall be Board Members or alternate Board Members and shall be designated by the Board, except that the Treasurer shall chair any Finance Committee. The Board shall attempt to appoint committee members in a manner that encourages diversity of representation on committees that reflects the diversity among Members. Committees shall be governed by the same rules regarding

meetings, action without meetings, notice, waiver of notice, and quorum (but not voting requirements) as applied to the Board; *provided that* meetings of the Operations Committee shall require such notice as required per Article VI, Section 6.8. The designation of any standing or special committee and the delegation to them of any authority shall not relieve the Board, or any Board Members of any responsibility imposed by law. No committee shall have the authority to take any action inconsistent with the Agreement, the Bylaws, or RCW 24.06.145.

Section 4.13 Agendas. Prior to each Executive Board meeting the Chair shall establish an agenda for the meeting. At the beginning of the meeting, any Board member may request that an item be added to the agenda, provided that, items requiring prior notice (See Section 4.7) shall not be so added unless all Board members are present and waive the requirement of notice and agree to entertain the action.

Section 4.14 Open Public Meetings. All meetings of the Board shall be open to the public as and to the extent required by the Agreement, the Open Public Meetings Act (Chap. 42.30 RCW) and other applicable law.

Section 4.15 Resignation; Removal. A Board member may be removed by the appointing agency (or agencies in the case of a Board member representing multiple Principals or Subscribers) which he or she represents, and an individual Board Member may personally resign at any time. Resignation shall be effective upon the Board Member or the appointing agency(s) delivering written notice to the Chair or, if the Chair is resigning, to the Vice-Chair.

Section 4.16 Vacancies. Any vacancy occurring in the Board shall be filled by the appropriate appointing agency or agencies (in event the Member represents multiple Principals or Subscribers).

Section 4.17. Compensation. All Board Members and their alternates shall serve without compensation; however, the PORTAL AGENCY may pay for or reimburse Executive Board Members and alternates for out-of-pocket costs related to service on the Executive Board.

ARTICLE V. OFFICERS

Section 5.1 Number. The PORTAL AGENCY shall have a Chair and a Vice-Chair, each of whom shall be elected by the Board. The Board shall also elect a Secretary and Treasurer or shall appoint same if non-Board Members are to fill these positions. Such other officers and assistant officers, as set forth in this Section 5.1 or as may be deemed necessary or appropriate may be appointed by the Board. The Chair shall preside at all meetings of the Executive Board

and shall have the additional responsibilities described in Section 5.4. The Vice-Chair shall serve as the Treasurer and Secretary of the Corporation during any times that a separate Treasurer or Secretary have not been appointed by the Board consistent with Section 7.l of the Agreement. Any two or more offices may be held by the same person, with the exception that the Chair and Vice-Chair, the Chair and Treasurer, or the Chair and Secretary may not be held by the same person.

Section 5.2 Election and Term of Office. The Chair and Vice-Chair initially shall be elected by Simple Majority Vote of the Board Members and shall serve through April 1, 2016, whereupon a new Chair and Vice-Chair shall be elected by the Board for a two-year term. Biennially thereafter, the Board shall elect a new Chair and Vice-Chair for two-year terms commencing each April 1. In the event of a vacancy in the Chair position, the Vice-Chair shall assume the Chair for the balance of the term of the departed Chair. In the event of a vacancy in the Vice-Chair position, the Executive Board shall elect a new Vice-Chair to serve the balance of the term of the departed Vice Chair. If the Treasurer and Secretary Officer positions are to be filled by Board Members, these positions shall be elected at the same time as the election of the Chair and Vice-Chair.

Section 5.3 Resignation. Any officer may resign at any time by delivering written notice to the Chair or by giving oral notice at any meeting of the Board. Any such resignation shall take effect at the time specified in the notice or, if the time is not specified, upon delivery of the resignation. Unless otherwise specified in the notice, the acceptance of a resignation shall not be necessary to make it effective.

Section 5.4 Chair (President). The Chair of the Executive Board (who shall be "President" under RCW 24.06.144 and for any required purposes) shall preside at all meetings of the Board and shall exercise and perform such other powers and duties enumerated below, and as may be determined from time to time by resolution of the Board. The Chair shall:

A. Preside at regular and special meetings and may call regular and special meetings of the Executive Board;
B. Select the site and agenda for all meetings;
C. Arrange for preparation and mailing or delivery of all meeting notices to Board member;
D. Arrange the maintenance and circulation of minutes of the meetings of the Board;
E. Act as the spokesperson for PORTAL AGENCY;
F. Execute documents on behalf of the Executive Board; and
G. Such other duties as identified in the Agreement and as may be delegated from time to time by the Executive Board.

In the absence of the Chair, or if there be none, the Vice-Chair shall preside at all meetings of the Board. The Chair may sign deeds, leases, bonds, Agreements, or other instruments which the Board has authorized to be executed, except in cases where the signing or execution thereof shall be expressly delegated by the Board or by these Bylaws to some other officer or agent of PORTAL AGENCY or shall be required by law to be otherwise signed or executed. In general, the Chair shall perform all duties incident to office of Chair and such other duties as may be prescribed by resolution of the Board.

Section 5.6 Vice-Chair. The Vice-Chair shall perform the duties of the Chair in the absence of the Chair. When so acting, the Vice-Chair shall have all the powers of and be subject to all the restrictions upon such officers and shall perform such other duties as from time to time may be assigned to the Chair by resolution of the Board.

Section 5.7 Secretary. The Vice-Chair, serving as Secretary, or a separately appointed Secretary, shall keep or cause to be kept, the minutes of the proceedings of the Board; shall give notices in accordance with the provisions of these Bylaws and as required by law; shall be custodian of the corporate records of the PORTAL AGENCY; shall have charge and custody of and be responsible for maintaining or overseeing maintenance of correct and complete nonfinancial books and records of the PORTAL AGENCY. The Secretary shall perform such other duties as from time to time may be assigned by resolution of the Board. If a person who is not a Board Member is appointed as Secretary, he/she shall not be considered an *ex officio* member of the Board.

Section 5.8 Treasurer. The Vice-Chair serving as Treasurer, or a separately appointed Treasurer, shall be responsible for maintaining, or overseeing maintenance of, all financial records of the PORTAL AGENCY, assuring the appropriate handling of all revenues and expenditures, and shall assist the Board in preparation of the annual budget. The Treasurer shall maintain or oversee maintenance of complete books and records of account, for all funds and securities of the PORTAL AGENCY, the transfer of receipts for money due and payable to the PORTAL AGENCY from any source whatsoever, and the deposit of all such money in the name of the PORTAL AGENCY in the banks, trust companies or other depositories as shall be selected in accordance with law. The Treasurer in general shall perform all duties incident to the office of Treasurer and such other duties as from time to time may be assigned to the Treasurer by resolution of the Board. If required by the Board, the Treasurer shall give a bond for the faithful discharge if his or her duties, in such sum and with such surety or sureties as the Board shall determine. If a person who is not a Board Member is appointed as Treasurer, he/she shall not be considered an *ex officio* member of the Board.

Section 5.9 Assistant Officers. The assistant officers, if any are appointed by the Board, shall in general perform such duties as are customary or as shall be assigned to them by resolution of

the Board. If required by the Board, the assistant Treasurers shall respectively give bonds for the faithful discharge of their duties in such sums and with such sureties as the Board shall determine.

Section 5.10 Delegation. In the case of absence or inability to act of any officer and of any person authorized to act in his/her place, the Board, by resolution, may, from time to time, delegate the powers or duties of such officer to any other officer or any Board Member or other person whom it may select. The Chair, by written notice to the Board, may delegate duties or powers, in addition to those listed, to officers of PORTAL AGENCY as necessary or appropriate to the conduct of the affairs of PORTAL AGENCY.

Section 5.11 Vacancies. Vacancies in any office arising from any cause may be filled by the Board at any regular or special meeting of the Board subject to the notice provisions set forth in Section 4.4 through 4.16 of the Bylaws.

Section 5.12 Indemnification. The PORTAL AGENCY shall indemnify officers and Board Members as set forth in the Articles of Incorporation.

ARTICLE VI. OPERATIONS COMMITTEE

Section 6.1 Powers. The Tax and Finance Operations Committee ("Operations Committee") shall have such powers, as described in Section 9 of the Agreement. No compensation shall be paid by the PORTAL AGENCY for any service as a Representative on the Operations Committee or as its Chair.

Section 6.2 Membership. Membership of the Operations Committee shall include one (1) Representative from each Principal, appointed by that Principal from time to time, plus at least one (1) representative, appointed by the Executive Board, to represent Subscribers. Each Principal shall also appoint in writing a designated alternate to serve on the Operations Committee in case of absence of the primary Representative**.**

Section 6.3 Qualification to serve on Operations Committee. Representatives and their alternates shall be staff from the Principal they represent, with expertise in city tax policy and administration and/or city financial policy and administration. Persons serving on the Operations Committee are referred to as Representatives (or alternates) and shall serve without compensation from the PORTAL AGENCY.

Section 6.4 Operations Committee Officers. The Operations Committee shall select an Operations Committee Chair and Vice-Chair from among the membership of the Operations Committee. It will be the function of the Operations Committee Chair to preside at the

meetings of the Operations Committee, and the Operations Committee Vice-Chair shall assume this role in absence of the Operations Committee Chair. The officers shall be initially elected at the first meeting of the Operations Committee following the effective date of this Agreement, by majority vote of the Representatives on the Operations Committee and shall serve through March 2016. Thereafter, the Operations Committee shall biannually elect an Operations Committee Chair and Vice-Chair for two-year terms beginning each April 1. In the event of a vacancy in the Chair position, the Vice-Chair shall assume the Chair for the balance of the term of the departed Chair. In the event of a vacancy in the Vice-Chair position, the Operations Committee shall elect a new Vice-Chair to serve to the balance of the term of the departed Vice-Chair. An officer of the Operations Committee elected to fill the unexpired term of his or her predecessor shall not be precluded from serving one or more full annual terms of office following the end of such unexpired term.

Section 6.5 Quorum. A quorum at any meeting of the Operations Board shall consist of Representatives of the Operations Committee (or their alternates) representing a simple majority of all members of the Committee. Representatives may attend meetings by telephone conference or equivalent means of voice communication.

Section 6.6 Voting. All actions and recommendations of the Operations Committee shall be approved by majority vote of those present and voting. Each Representative shall have one vote. No proxy votes shall be allowed. There shall be no weighted voting.

Section 6.7 Staffing. The Operations Committee shall be staffed by the Portal Agency Manager and such additional agency staffing as the Manager may deem appropriate.

Section 6.8 Meetings. The Operations Committee shall meet not less than once every calendar quarter, at a time and place designated by the Chair of the Operations Committee or by a majority of its Representatives. Not less than ten (10) days advance notice of regular meetings shall be given. Special meetings may be called by the Chair of the Operations Committee or Representatives representing at least two or more members of the Committee representing at least two different Principals and upon giving all other Representatives not less than seven (7) days prior notice of such meeting. In an emergency, the Operations Committee may dispense written notice requirements for special meetings, but must, in good faith, implement best efforts to provide fair and reasonable notice to all Representatives. Representatives (or alternates) may participate in meetings by telephone conference or other equivalent means of voice communication.

Section 6.9 Additional Rules. The Operations Committee may adopt additional rules for its operations that are not inconsistent with the Agreement or these Bylaws.

ARTICLE VII. STAFF AND CONSULTANTS

The staff of PORTAL AGENCY shall consist of the Manager and such other staff positions established by the Board. The Board shall appoint the Manager, pursuant to the provisions of the Agreement. The Manager shall appoint persons to fill other staff positions, subject to such confirmation by the Board as the Board may require. Only the Board shall be authorized to hire or retain legal counsel and independent accountants and auditors. Other consultants may be designated in such manner as the Board may determine, subject to Sections 6 and 7 of the Agreement.

ARTICLE VIII. EXECUTION OF AGREEMENTS AND OTHER INSTRUMENTS

Execution of Agreements and Deeds. Except as otherwise provided by resolution of the Board authorizing the execution thereof, all agreements, deeds, leases, transfers and other written instruments binding upon the PORTAL AGENCY for amounts involving the expenditure of greater than $50,000, shall be executed on behalf of the PORTAL AGENCY by the Chair and one other officer. The execution of documents involving amounts less than $50,000 may be signed by the PORTAL AGENCY Manager alone, after advising the Board.

ARTICLE IX. FINANCES

Section 9.1 Loans. The PORTAL AGENCY is not authorized to issue debt. No loans shall be made by the PORTAL AGENCY to any officer, Board Member or private entity, nor shall loans be made in violation of the Washington State Constitution or applicable law.

Section 9.2 Checks, Drafts, Warrants, Orders and Credit Cards. All checks, drafts, warrants, credit cards, debit cards or other orders for the payment of money or issued in the name of the PORTAL AGENCY shall be signed by officers of the PORTAL AGENCY or the Manager subject to such limits and in the manner as shall from time to time be prescribed by resolution of the Board and consistent with law applicable to Washington State local government entities. In the absence of such provision by the Board such instrument shall be signed by any two officers of the PORTAL AGENCY, one of whom shall be the Vice-Chair. Use of credit cards by PORTAL AGENCY shall be in compliance with RCW 43.09.285.

Section 9.3 Contributions and Disbursements. All contributions and other funds received by PORTAL AGENCY shall be deposited in a special account or accounts in such banks, trust companies or other depositories as the Board may select. All disbursements shall be made under proper authority of the Board. All contributions, income to and disbursements of

PORTAL AGENCY shall be recorded by the Vice-Chair's (or Treasurer's) designee in appropriate books and records and such records shall be subject to examination at any reasonable time, upon request by any director.

Section 9.4 Budget/Financial Management. An annual budget of proposed receipts, operating income and expenditures shall be prepared by the Manager and submitted to the Board for its approval by May 1 prior to the beginning of the fiscal year in which that budget will take effect, and if not so timely submitted, the Vice-Chair (or Treasurer) shall submit a budget to the Board for its approval as soon as practicable after such date. The budget shall identify the level of rates and charges upon which revenue projects are based. When finally approved by the Board after action by Principals per the Agreement, such budget shall be the authorization for expenditures and operating expenses of the PORTAL AGENCY, subject to subsequent changes in such budget made by the Board.

Section 9.5 Expenditures for Qualifying Purposes Only. Subject to applicable law, the funds of the corporation may be expended or distributed only for the purposes of the PORTAL AGENCY as described in the Agreement and in the Articles of Incorporation.

ARTICLE X. ETHICS

The PORTAL AGENCY, its Board Members, committee members and employees (including loaned staff) shall be subject to and comply with the requirements of Ch. 42.23 RCW ("Code of Ethics for Municipal Officers – Contract Interests") as the same may be amended or replaced from time to time.

ARTICLE XI. SEAL

The PORTAL AGENCY need not have a corporate seal. If the Board adopts a corporate seal, the seal of the PORTAL AGENCY shall be circular in form and consist of the name of the Washington Multi-City Business License and Tax Portal Agency, the state and year of incorporation, and the words "Corporate Seal."

ARTICLE XII. BOOKS AND RECORDS

The PORTAL AGENCY shall keep correct and complete books and records of account, minutes of the proceedings of the Board, and any committees designated by the Board, and such other

records as may be necessary or advisable. All books and records shall be subject to disclosure under the Public Records Act, Chapter 42.56 RCW.

ARTICLE XIII. COPIES OF RESOLUTIONS

Any person dealing with the PORTAL AGENCY may rely upon a copy of any of the records of the proceedings, resolutions or votes of the Board when such records are certified by the Vice- Chair or Secretary, if a separate Secretary is appointed.

ARTICLE XIV. AMENDMENTS TO BYLAWS.

These Bylaws may be adopted, altered, amended or repealed, and new Bylaws may be adopted, all by Supermajority Vote of the Board.

The undersigned, being the Chair and Vice-Chair of the PORTAL AGENCY, hereby certified that these Bylaws are the Bylaws of the PORTAL AGENCY, adopted by Resolution No. 2014-_____of the Board on__, 2014.

Dated this____day of_____, 2014.

_____
Chair

_____
Vice-Chair

APPENDIX B: ORGANIZATIONAL CHART, ROSTER

Washington State Municipalities
Governing Board - Executive Board

City of Bellevue	Toni Call
City of Des Moines	Beth Anne Wroe
City of Everett	Susy Haugen
City of Lake Forest Park	Lindsey Vaughn
City of Renton	Jan Hawn
City of Seattle	Glen Lee
City of Tacoma	Andy Cherullo

Washington State Municipalities
Governing Positions

City of Seattle	Glen Lee	Chair
City of Tacoma	Andy Cherullo	Vice-Chair
Francis and Company	Horace Francis	Treasurer
FileLocal Agency	Julie Panick	Secretary

Washington State Municipalities
Governing Board - Executive Board Alternates

City of Bellevue	Jamie Robinson
City of Des Moines	Shawn Hunstock
City of Everett	Sharon Fuller
City of Lake Forest Park	Aurora Belli
City of Renton	Kari Roller
City of Seattle	Joseph Cunha
City of Tacoma	Susan Ramirez

Washington State Municipalities
Governing Board - Operations Committee

City of Bellevue	Troy Lucas
City of Des Moines	Shawn Hunstock
City of Everett	Anna Pankovich
City of Lake Forest Park	Lindsey Vaughn
City of Renton	Nate Malone
City of Seattle	Joseph Cunha
City of Tacoma	Danielle Larson

Washington State Municipalities
FileLocal Agency

Program Manager	Kevin Fitzpatrick
Project Manager	Wendy Thomaston
Program Assistant	Julie Panick

Washington State Municipalities
Technical Service Vendors

Software as a Service	Avenu Insights
Payment Processing	Kubra Data Transfer LTD.
Information Security	Leviathan Security Group

Washington State Municipalities
Professional Service Vendors

Accounting	Francis and Company
Legal	Madrona Law

FL2019-09 Attachment C

AUTHORITIES DELEGATED BY FILELOCAL EXECUTIVE BOARD	TOPIC	DOCUMENTATION	PROGRAM MANAGER	OPERATIONS COMMITTEE	OTHER	ACCOUNTANT	LEGAL
Authorizes budgeted expenditures of $50,000 or less - excluding Program Manager (PM) requests.	F	(FM §6.1)	X				
Authorizes budgeted expenditures of more than $50,000 - excluding PM requests .	F	(FM §6.1)			X		
Authorizes unbudgeted expenditures of $5,000 or less-excluding PM requests .	F	(FM §6.1)			X		
Authorizes unbudgeted expenditures of more than $5,000-excluding PM requests.	F	(FM §6.1)			X		
Contract Review >$5,000	F	(FM §6.1)			X		
Authorizes all budgeted PM requests $5,000 or less.	F	(FM §6.1)			X		
Authorizes all budgeted PM requests greater than $5,000.	F	(FM §6.1)			X		
Authorizes all unbudgeted PM requests $2,000 or less.	F	(FM §6.1)			X		
Authorizes all unbudgeted PM requests greater than $2,000.	F	(FM §6.1)			X		
Assist in Development and review proposed agency budgets	F	(FM §3)		X			
Advises on proposed budget	F	(FM §3)	X				
Develops proposed operating budget in consultation with operations committee	F	(FM §3)	X				
Submits budget and operation performance reports to Board	F	(FM §1)	X				
Reviews/approves cash disbursements	F	(FM, §6.2)	X				
Prepares checks, maintains and initiates electronic payments	F	(FM, §6.2)				X	
Reviews bank accounts and reconciliations	F	(FM, §6.2)				X	
Approves check requests (as authorized by Executive Board)	F	(FM, §6.3)				X	
Controls check stock	F	(FM, §6.4)				X	
Establishes and maintains accounting system	F	(FM, §2)				X	
Preparation of financial statements	F	(FM, §11)				X	
Provides external audit preparation and response	F	(FM, §6.11)				X	
Conducts compliance monitoring, financial analysis, internal audits, and other financial management and accounting services as directed by Board	F	(FM, §6.11)				X	

Legend	
F=Fiscal	ILA=Interlocal Agrement
O=Operations	B=Bylaws
P=Policy	SLA=Service Level Agreement
FM=Fiscal Manual	

FL2019-09 Attachment C

AUTHORITIES DELEGATED BY FILELOCAL EXECUTIVE BOARD	TOPIC	DOCUMENTATION	PROGRAM MANAGER	OPERATIONS COMMITTEE	OTHER	ACCOUNTANT	LEGAL
Provides legal services regarding formation as a non-profit municipal corporation	L	(FL2014-18)					X
Provides general legal counsel	L	(FL2014-18)					X
Manages/oversees vendor performance	O	(ILA §11)	X				
Consults with Operations Committee on issues coming before Board	O	(ILA §11)	X				
Provide, equip, and maintain office space for staff	O	(FL2014-19)			X COS		
Reviews and develops operations policy and amendments, new service options, and other matters directed by Board	P	(ILA §9)		X			
Reports and recommends on policy matters deemed appropriate	P	(ILA §9)		X			
Assists in communications to City Councils, legislators, business community, etc.	Policy	(ILA 16-17)		X			
Conducts outreach to tech staff within respective cities	Policy	(ILA 16-17)		X			
Briefs executive board members	Policy	(ILA 16-17)		X			
Administers day-to-day operations consistent with policies	Policy	(ILA 18)	X				
Conducts outreach to taxpayers, licenses and businesses	Policy	(ILA 18)	X				
Advise on conflicts of interest	Policy	(SLA, p4)			X SEEC		
Preserves agency public records as required by state law, response to public records requests, segregation of agency records from city records	Policy	(SLA, p5)	X		X Seattle		
Outreach and communications with elected officials	Policy				xOIR		
Appoints other staff positions established by Board	Staffing	(B p9)	X				
Appoints persons to fill other staff positions (Administrative support staff, project manager/business analyst, etc.)	Staffing	(ILA 18, SLA 3)	X				
Backfills employees	Staffing	(SLA, p4)			X Seattle		

Legend

F=Fiscal	ILA=Interlocal Agrement
O=Operations	B=Bylaws
P=Policy	SLA=Service Level Agreement
FM=Fiscal Manual	

Executive Board Meeting Schedule

Executive Board meeting schedules are approved via a resolution passed by the Board. All meetings are held at the Seattle Municipal Tower (SMT) and are open to the public.

Year	Type	Date	Time	Location
2020	Special	Feb 24, 2020	11:00am – 12:00pm	SMT 4090
	Regular	Mar 19, 2020	CANCELLED	SMT 4086
	Regular	Apr 17, 2020	11:00am – 12:00pm	Conference Call
	Regular	May 28, 2020	11:00am – 12:00pm	Conference Call
	Regular	Sep 30, 2020	11:00am – 12:00pm	Conference Call
	Regular	Dec 17, 2020	11:00am – 12:00pm	Conference Call
2019	Regular	Mar 28, 2019	11:00am – 12:00pm	SMT 4070
	Regular	May 30, 2019	11:00am – 12:00pm	SMT 4070
	Regular	Sept 26, 2019	11:00am – 12:000m	SMT 4070
	Regular	Dec 19, 2019,	11:00am – 12:00pm	SMT 4070
2018	Special	Mar 19, 2018	11:00 am – 12:00 pm	SMT 4240
	Annual	Mar 26, 2018	12:00 pm – 1:00 pm	SMT 4070
	Regular	May 29, 2018	12:00 pm – 1:00 pm	SMT 4090
	Regular	Sep 24, 2018	12:00 pm – 1:00 pm	SMT 4070
	Regular	Dec 10, 2018	12:00 pm – 1:00 pm	SMT 4070
2017	Special	Feb 6, 2017	2:00 pm – 2:30 pm	SMT 4240
(via FL2016-12)	Annual	Mar 27, 2017	12:00 pm – 1:00 pm	SMT 4070
	Regular	Jun 12, 2017	12:00 pm – 1:00 pm	SMT 4070
	Regular	Sep 25, 2017	12:00 pm – 1:00 pm	SMT 4070
	Regular	Dec 11, 2017	12:00 pm – 1:00 pm	SMT 4070
2016	Special	Jan 19, 2016	11:00 am – 12:00 pm	SMT 4080
(via FL2016-01)	Regular	Jan 25, 2016	12:00 pm – 1:00 pm	SMT 4070
	Annual	Mar 28, 2016	12:00 pm – 1:00 pm	SMT 4070
	Regular	May 23, 2016	12:00 pm – 1:00 pm	SMT 4070
	Special	Jun 3, 2016	12:00 pm – 1:00 pm	SMT 4090
	Special	Jun 27, 2016	10:00 am – 11:00 am	SMT 4070
	Regular	Sep 26, 2016	12:00 pm – 1:00 pm	SMT 4070
	Special	Nov 18, 2016	10:30 am – 11:00 am	SMT 4090
	Regular	Dec 12, 2016	12:00 pm – 1:00 pm	SMT 4070
2015	Special	Jan 26, 2015	12:00 pm – 1:00 pm	SMT 4070
(via FL2015-01)	Annual	Mar 23, 2015	12:00 pm – 1:00 pm	SMT 4070
	Regular	Apr 27, 2015	12:00 pm – 1:00 pm	SMT 4070
	Special	May 14, 2015	CANCELLED	
	Regular	May 26, 2015	11:30 am – 1:30 pm	SMT 4070
	Regular	Jul 27, 2015	12:00 pm – 1:00 pm	SMT 4070
	Regular	Sep 28, 2015	12:00 pm – 1:00 pm	SMT 4070

Executive Board Meeting Schedule

	Regular	Dec 14, 2015	12:00 pm – 1:00 pm	SMT 4070
2014	Annual	Mar 24, 2014	12:00 pm – 1:00 pm	SMT 4070
(via FL2014-03)	Regular	Apr 28, 2014	12:00 pm – 1:00 pm	SMT 4070
	Regular	May 27, 2014	9:00 am – 10:00 am	SMT 4070
	Regular	Jun 23, 2014	**CANCELLED**	
	Special	Jul 16, 2014	2:00 pm – 4:00 pm	SMT 4090
	Regular	Sep 22, 2014	12:00 pm – 1:00 pm	SMT 4070
	Regular	Dec 15, 2014	12:00 pm – 1:00 pm	SMT 4070

FileLocal

Your one stop for local business licensing and tax filing

www.filelocal.org

OPERATIONS POLICIES & PROCEDURES

~~May 2018~~

TABLE OF CONTENTS

Introduction

Purpose 3

Overview 3
Guiding Principles 3
Business Structure 4

Roles, Rules and Responsibilities

Executive Board Meetings 5
Executive Board Membership, Terms, Quorum, Voting 5
Overview of Roles and Responsibilities 6

Operational Procedures

Communications Protocols ..... ~~8~~7
Conflict of Interest Policy ..... ~~12~~11
Emergency Procedures 20
Fiscal Manual 21
Information Technology Securities Policy Manual ..... ~~44~~46
Public Records Policy 102
Use of Electronic Signatures 107

Appendices

A. Key Governance Documentation 108
A1. Articles of Incorporation 109
A2. Interlocal Agreement 119
A3. Bylaws 165
B. Organizational Chart, Roster 178
C. Delegation of Authorities 179
D. Executive Board Meeting Schedules 181

Introduction

Purpose

The FileLocal Operations Manual has several purposes: to help guide FileLocal leaders, staff and city partners in developing and sustaining a successful enterprise; to document procedures and policies; to support agency accountability and efficiency; and to serve as a reference for questions and problems as they arise in day-to-day operations.

Overview

FileLocal's primary purpose is to offer a web-based service that will make it easier for businesses to obtain a business license and pay local taxes to its member cities.

FileLocal is a municipal corporation authorized by state law to issue local business licenses and collect a variety of local taxes. It was formed to make it easier and more efficient for businesses to apply for local business licenses and file local taxes while allowing cities to retain local control over licensing and tax collection functions and policies. The Principal cities – Bellevue, Everett, Seattle, and Tacoma – jointly facilitated the creation of an internet web application gateway (a "portal") where tax collection and business licensing functions can be collectively administered, and where businesses operating in multiple cities can use a "one-stop" system for tax payment or business license application filing.

Guiding Principles

The principles guiding FileLocal reflect integrity, accountability, local control, flexibility, accessibility, security, and affordability for cities, businesses, and taxpayers:

- Integrity: FileLocal will be honest, truthful, and straightforward.
- Accountability: FileLocal will be responsible for its actions and decisions, a good steward of public funds and transparent in its operations.
- Local Control: FileLocal will seek to respect and preserve each participating city's authority to set local tax policies.
- Flexibility: FileLocal will strive to nimbly respond to a changing business, technology, and policy environment.
- Accessibility: FileLocal will seek to be accessible and responsive to taxpayers, licensees,

and participating cities.

- Security: FileLocal will at all times seek to safeguard taxpayer, licensee, and participating city data.
- Affordability: FileLocal will seek to be affordable to both Participating Cities and businesses and taxpayers using the portal. Also, fees and charges will be structured so that the addition of new cities using the portal does not impose additional costs on prior participating cities.

Business Structure

FileLocal is a public agency formed as a nonprofit corporation as authorized by the state Interlocal Cooperation Act (39.34 RCW) and the Nonprofit Misc. & Mutual Corporations Act (24.06 RCW). FileLocal is an instrumentality of its member cities formed to carry out exclusively governmental activities. The four founding cities are Bellevue, Everett, Seattle, and Tacoma. The legal name of the agency is the "Washington Multi-City Business Licenses and Tax Portal Agency."

The four founding cities are the "Principals" and have representation on the Executive Board, which governs the agency. Additional Washington cities may apply to join FileLocal, either as a Principal or as a Subscriber. Principals have voting rights on the Executive Board; Subscribers have nonvoting representation on the Executive Board.

Roles, Rules, and Responsibilities

EXECUTIVE BOARD MEETINGS

All Meetings will be held at the Seattle Municipal Tower (SMT) and via Skype. These meetings are open to the public in compliance with the Washington State Open Public Meetings Act (42.30 RCW). Meeting dates, times, locations, materials, and summaries are posted on filelocal.org. Unless otherwise noted, meetings are held in SMT 4070 at 12:00 pm. Skype meeting information is for Board members only; the public must attend in person.

EXECUTIVE BOARD MEMBERSHIP, TERMS, QUORUM, VOTING

This document is meant to be a summary of the more detailed descriptions provided in the FileLocal ILA and Bylaws.

MEMBERSHIP

- The FileLocal Board consists of one representative from each Principal city
- Individuals must be a Chief Financial Officer or their deputy or equivalent
- Alternates are designated in writing and must meet same qualifications

TERMS

- Unless the member resigns or is removed in accordance with the Bylaws, each member holds office until replaced by resolution or written motion of the legislative body of the appointing Principal
- Board members representing multiple principals are selected biennially

QUORUM

- A simple majority of members (or their alternates)

VOTING

- Each member has one vote
- A "Supermajority Vote' means Executive Board approval of an item accomplished by securing affirmative votes of not less than sixty-six percent (66%) of all voting Board Members of the Executive Board in number, and not less than sixty-six percent (66%) in number of the Original Principals (the Cities of Bellevue, Everett, Seattle, and Tacoma) [i.e., 3 out of 4]. Generally, items requiring supermajority vote for approval involve the following:
  - Budget, user fees/charges
  - Operations policies

- Major docs: Bylaws, Articles of Incorporation, ILA
- Decisions with significant financial impact (e.g., contracts over $50,000)
- Adding or removing people (New principals or subscribers, adding seats, adding staff positions, removing the manager)
- Merging, sale, dissolving

Table 1:OVERVIEW OF ROLES AND RESPONSIBILITIES

PRINCIPAL CITIES	ROLE: Incorporators
Accountable to	Voters

EXECUTIVE BOARD	ROLE: Governing Body
Accountable to	State, pursuant to Interlocal Cooperation Act (39.34 RCW)
Responsibilities	• Final decision-making authority on policy issues • Recommending action to participating city legislative bodies • Review/approve budget and budget policies • Review/adopt personnel, operating, financial policies • Direct/supervise committees/advisory boards • Conduct regular and special meetings • Manage/maintain records • Determine services offered/ terms • Approve new principals and subscribers • Establish fund or special funds Retain/terminate manager • Create committees • Enter into agreements • Establish fees • Approve strategic plans • Accept funds • Receive property (et. al.) • Sue and be sued • Make/alter bylaws

OPERATIONS COMMITTEE	ROLE: Advise and Recommend
Accountable to	Executive Board
Responsibilities	• Assist in review/development of operations policy, development options, proposed new services, other matters as directed • Provide advice, information, and recommendations to staff • Assist in review/development of budget • Assist in communications • Reach out to tech staff within cities • Brief Executive Board members

PROGRAM MANAGER	ROLE: Manage Agency
Accountable to	Executive Board
Responsibilities	• Ensure overall compliance of agency with laws and regulations • Management of staff and technology vendors • Quality control and operations of portal • Administrative support of board • External relations

LEGAL	ROLE: Legal Counsel
Accountable to	Executive Board and Program Manager
Responsibilities	Review resolutions and contracts; ensure legal compliance

ACCOUNTING	ROLE: Financial Compliance
Accountable to	Executive Board and Program Manager
Responsibilities	Prepare and manage financial reports; support audits as required

TECHNOLOGY VENDORS	ROLE: Portal Technological Management
Accountable to	Program Manager
Responsibilities	Manage portal, handle payments, ensure information security

COMMUNICATIONS	ROLE: Manage City Communications
Accountable to	Executive Board
Responsibilities	Manage city's communications and coordinate with other cities on joint communications

INTERGOVERNMENTAL RELATIONS	ROLE: Lobbyists
Accountable to	Executive Board
Responsibilities	Lobby state government legislators on behalf of cities and agency

Communications Protocols

1. Purpose

Ensuring that taxpayers and the general public receive timely and accurate information regarding FileLocal is a communication priority. The FileLocal staff and cities are charged with communicating with external audiences about FileLocal. The FileLocal program manager coordinates communications and relies on partner cities' communication resources. Effective communication requires strategic direction, coordination and clear roles and responsibilities.

2. Policy

All parties commit to act in good faith in seeking to work together in an open and forthright manner. Communications between the parties will be early and frequent to guarantee strong coordination, maximize opportunities and minimize surprises. The public will not typically distinguish between FileLocal and the individual cities. It will benefit all parties to work cooperatively to inform the public that we are effectively and safely providing the level of services people expect and deserve.

FileLocal and the cities will coordinate communications to ensure:

A. Timely information is easily accessible to businesses and the public.

B. Communication goals are met.

C. Messages are consistent.

D. Appropriate credit is shared.

3. Background

- FileLocal offers a web-based service that will make it easier for businesses to obtain a business license and pay local taxes, for multiple cities, from one website
- FileLocal is a municipal corporation authorized by state law to issue local business licenses and collect a variety of local taxes.
- FileLocal makes it easier and more efficient for businesses to apply for local business licenses and file local taxes while allowing cities to retain local control over licensing and tax collection functions and policies.
- The Principal cities – Bellevue, Everett, Seattle, and Tacoma – jointly facilitated the creation of FileLocal.

4. Roles

- The FileLocal Program Manager is the communications lead, primary spokesperson, and media contact for FileLocal. The Program Manager is

provided through a Service Level Agreement between the City of Seattle and FileLocal. If the Program Manager is not available, the role defers to the FileLocal Executive Board Chair~~.~~

~~o Kevin Fitzpatrick (FileLocal, Program Manager)~~

~~o Susy Haugen (Executive Board Chair)~~

- (Reference Appendix B).

- An Executive Board (Board) governs FileLocal (a not-for-profit corporation under Washington law, formed as Washington Multi-City Business License and Tax Portal Agency). As such, it provides leadership and overall direction on FileLocal communications. The Board is comprised of four ~~four~~ seven directors, representing each of the principal cities (Reference Appendix B)

~~• directors, representing each of the Principal cities:~~

~~•~~

  - ~~Toni Call (Finance Director,~~ City of Bellevue~~)~~
  - ~~Susy Haugen (Treasurer,~~ City of Des Moines
  - City of Everett~~ | Executive Board Chair)~~
  - ~~Glen Lee (Finance Director,~~ City of Lake Forest Park
  - City of Renton
  - City of Seattle~~)~~
  - ~~Andy Cherullo (Finance Director,~~ City of Tacoma ~~| Executive Board Vice-Chair)~~

~~• City communications staff provide on-the-ground communications support.~~

~~o David Grant (Public Information Officer, City Manager's Office, City of Bellevue)~~

~~o Meghan Pembroke (Public Information Director, City of Everett)~~

~~o Julie Moore (Communications Director, FAS, City of Seattle)~~

~~o Gwen Schuler (Media and Communications Manager, City of Tacoma)~~

- FileLocal's technical providers (vendors) are ~~e-Gov~~Avenu, KUBRA, and Leviathan.

~~• City Intergovernmental Relations staff also support the project.~~

~~o Joyce Nichols (City of Bellevue, jnichols@bellevuewa.gov)~~

~~o Doug Levy (City of Everett, levy4@msn.com)~~

~~o Caron Cargill (City of Seattle, caron.cargill@seattle.gov)~~

~~o Randy Lewis (City of Tacoma, rlewis@cityoftacoma.org)~~

~~o Brihna Taylor (City of Tacoma, btaylor@gth-gov.gov)~~

~~o Serena Dolly (Association of Washington Cities, serenade@awcnet.org)~~

~~o Victoria Lincoln (Association of Washington Cities, victorial@awenet.org)~~

5. Protocols

A. The following protocols serve as guidelines for communicating effectively with external audiences. The protocols are intended to be fluid – capable of reacting to feedback and changes as needed. The protocols should be reviewed regularly to

ensure that they are effective and appropriate as needs change. Activities include, but are not limited to:

I. Providing information to businesses/citizens/public
II. Providing information to other cities/units of government
III. Meeting requests and correspondence
IV. Media relations
V. Materials, including content development and production of digital, print, ~~signage and~~ signage and identity
VI. Coordination with the public, agencies, consultants, vendors, etc.

B. External communications with the public, stakeholders and the media will be coordinated by the FileLocal Program Manager to leverage resources, ensure accuracy of information and to minimize surprises. City/Executive communication staff will be included in information sharing so that they are prepared to respond.

C. As the governing body, the FileLocal Board will review policy, finance, and planning-related communications.

D. As the service provider, the Program Manager will lead operations-related communications. This includes but is not limited to communications related to:

I. Project preparation, testing, launch, and maintenance
II. Ongoing services
III. Operations, contractors, and personnel

E. Service incident protocols are being developed by ~~e-Gov~~Avenu. Please refer to these separate protocols for additional detail.

F. Production of materials will be coordinated and reviewed by the Program Manager to ensure accuracy.

I. The FileLocal logo will be included on all communication materials. Principal city logos should only be added when the material reflects a jointly sponsored event.

II. Boilerplate language agreed upon by all parties describing the relationship between the cities and FileLocal will be included. (FileLocal is an easy and flexible online tool that provides a streamlined approach to applying for business licenses and filing local taxes with any Washington member city.)

III. Development of materials will be assigned appropriately to utilize expertise and leverage resources efficiently. The lead entity will be responsible for generating first drafts of materials.

IV. All drafts will be reviewed and approved by the Program Manager before distribution.

V. Every effort to provide reasonable review time will be provided (taking into account unforeseen circumstances or constraints). Similarly, timely approval of materials is expected.

G. Contacts will be alerted of all media contacts and meeting requests and be provided a brief summary of the interaction in a timely manner.

I. Reporter or organization name and contact information

II. Summary of the request and deadline

III. Coordination between FileLocal and cities on appropriate and available spokesperson

IV. Follow-up to confirm reporter or organization has received a response

H. FileLocal will maintain project information on its website. It will work with cities to coordinate web sites and minimize duplication and confusion.

I. The FileLocal site will include governance, policy, and planning issues.

II. Cities will include a banner or icon on their websites that links to FileLocal. They will not duplicate or maintain FileLocal information on city websites.

I. Every effort will be made to maintain clear and timely internal communications between FileLocal and its partner cities. This includes, at a minimum, quarterly communication meetings between FileLocal and city communicators and regular reports from the Project Manager to the FileLocal Board.

6. Key Contacts (Reference Appendix B)

FileLocal

~~Kevin Fitzpatrick~~ Program Manager ~~http://filelocal.org/~~
~~kevin.fitzpatrick-flo@seattle.gov~~

PO Box 94669, Seattle, WA 98124
206-233-2513

Principal Cities

City of Bellevue

City of Des Moines

City of Everett

City of Lake Forest Park

City of Renton

City of Seattle

City of Tacoma

~~Julie Moore~~
~~Communications Director, FAS~~
~~City of Seattle~~
~~julie.moore@seattle.gov~~
~~206-684-0480 direct~~
~~206-684-0909 media~~

~~Meghan Pembroke~~
~~Public Information Director~~
~~City of Everett~~
~~mpembrok@everettwa.gov~~
~~425-257-8687 office~~
~~425-418-0936 cell~~

~~David Grant~~
~~Public Information Officer~~
~~City Manager's Office~~
~~City of Bellevue~~
~~dgrant@bellevuewa.gov~~
~~425-452-4397 office~~
~~206-450-5432 cell~~
~~425-452-5247 fax~~

~~Gwen Schuler~~
~~Media and Communications Manager~~
~~City of Tacoma~~
~~gwen.schuler@cityoftacoma.org~~
~~253-591-5160 office~~
~~253-365-0463 cell~~

7. Conflict Resolution

It is the intent of all parties to act in good faith on all matters. Should a dispute arise between the FileLocal Board, Program Manager, Vendor and/or cities over any of the agreed upon protocols or related to communications, the FileLocal Board Chair and Program Manager will be the main points of contact.

The parties shall seek in good faith to resolve any such dispute or concern by meeting, as soon as feasible. The meeting shall include the Chair of the Executive Board, the Program Manager, and not more than two (2) representatives of the City with positional authority to negotiate and resolve the dispute.

Conflict of Interest Policy

1. Purpose

The purpose of this policy is to establish guidelines for ethical standards of conduct to govern Washington Multi-City Business License and Tax Portal Agency board members, agency staff, and any employees (hereafter referred to as Agency officials) in the performance of Agency business and the duties of their respective jobs. This policy is intended to provide positive direction in order to prevent potential conflicts of interest. This policy is not all encompassing in its definition of conflict of interest. Action deemed inappropriate by a reasonable person, whether specifically cited in this policy or not, shall be subject to inquiry under this policy.

2. Definitions

The following definitions shall apply for purposes of this policy:

A. “Agency official” is any Agency staff, Board member, or employee as defined below.

B. “Agency staff” is any employee provided under a loaned staff agreement.

C. "Board member" or “Executive Board” member is the individual representing a principal on the Executive Board, whether the Chief Financial Officer of such principal or his/her designated alternate.

D. "Business" is any corporation, partnership, sole proprietorship, firm, enterprise, franchise, self- employed individual, consultant, holding company, joint-stock company, receivership, trust, or any legal entity organized for profit.

E. "Employee" is a person or persons employed on a full-time continuing basis by the Agency and, for the purpose of this policy only, and shall include part-time, intermittent, or temporary workers. The term shall not include employees of Seattle who provide services or perform duties for the Agency pursuant to interlocal agreement, loaned staff agreement, between the Agency and Seattle. The term shall not include persons engaged or retained by the Agency pursuant to contract to perform consulting or special technical services.

F. "Gift" is anything of economic value, but shall not include campaign contributions regulated by the provisions of chapter 42.17A RCW, informational materials exclusively for official or office use, memorials, trophies and plaques of no commercial value.

"Immediate family" is an Agency official’s spouse, domestic partner, child or the child of an Agency official’s domestic partner, and other dependent relatives if living in his or her household.

G. "Interest" is any direct or indirect monetary or material benefit accruing to an Agency official as a direct result of contracts or transactions which are or may be the subject of an official act or action by or with the Agency, except contracts or transactions which confer similar benefits to all other persons and/or property similarly situated. An Agency official shall not be deemed to have an interest in conflict with his or her official duties for purposes of this code if the interest is remote

"Remote interest" means:

i. That of a non-salaried officer of a nonprofit corporation;

ii. That of a landlord or tenant of a contracting party; or

iii. That of a creditor, debtor or ownership interest of less than one thousand five hundred dollars in a business entity which is a contracting party or as a holder of less than one percent of the shares of a corporation or cooperative which is a contracting party, whichever is less.

H. "Program Manager" is the chief operating officer for the Portal Agency appointed by and serving at the pleasure of the Executive Board.

3. Background

In keeping with the policies declared by the State Legislature in enacting codes of ethics for municipalities, it is recognized that high moral and ethical standards among public officials and employees are essential to the conduct of government. A code of ethics for the guidance of Agency officials is necessary in order to avoid and prevent conflicts of interest in public office, to improve standards of public service and to promote and strengthen the faith and confidence of the citizens in the Agency. Agency officials are, therefore, obligated to treat their offices and duties as a public trust, using their official powers and duties and the resources of the Agency only to advance the public interest. It is expected that Agency officials will conduct their public and private actions and financial dealings in a manner that will present no actual or apparent conflict of interest between the public trust and their private interests.

This obligation requires that all Agency officials devote their best efforts and attention to:

A. Being independent and impartial in the exercise of their duties and avoiding actions that create even the appearance of using their positions for personal gain or private benefit.

B. Strengthening public confidence in the integrity of the Agency's decisions by demonstrating the highest standards of personal integrity, fairness, honesty, and compliance with both the spirit and the letter of the law and this resolution.

C. Creating a work environment that is free from all forms of unlawful discrimination and harassment.

D. Managing human and environmental resources for the benefit and enjoyment of both current and future generations.

E. Conducting the public's business openly and, to the maximum extent consistent with existing law, resolving doubtful cases in favor of public access.

F. Serving the public with respect, concern, courtesy, and responsiveness, recognizing that service to the public is the primary mission of government.

G. Promoting an environment of public trust free from fraud, abuse of authority and misuse of public property.

H. Protecting the integrity of the decision-making process by recognizing and avoiding conflicts between public duties and private interests and activities.

I. Respecting and protecting privileged information to which Agency officials have access in the course of their official duties including, but not limited to, information provided in lawful executive sessions of the Board.

4. Policies and Procedures

A. Gifts

No Agency official shall accept any gifts.

B. Use of Agency Property

No Agency official shall request, use, or permit the use of Agency-owned vehicles, equipment, materials, or property for personal convenience or profit. Use is to be restricted to such services as are available to the public generally and for the conduct of official business.

C. Procurements

I. The Agency intends to conduct its procurements of work and for professional services with integrity, fairness, and openness. Agency officials involved in Agency procurements shall not act or fail to act in any way which compromises the fairness of Agency procurements or which creates actual or apparent conflicts of interest. Agency officials are expected to use good judgment and to act in accordance with Agency policies, policies of the member jurisdiction, applicable laws, and the best interests of the Agency. The Program Manager for the Agency shall be the focal point for receiving and responding to communications from the public, potential bidders or proposers and other government staff and Board members concerning the procurement unless otherwise approved by the Board.

II. Agency officials directly involved in an Agency procurement process shall promptly identify any past or current personal, financial, or business relationship with any firm, or principals associated with a firm, which submits bids or proposals to the Agency. Disclosure shall be made to the Program Manager for the Agency. Determination of the appropriate response, if any, shall be made by the Program Manager of the Agency with advice of legal counsel.

III. In the event a Board member receives information or requests for information from the public, potential bidders or proposers or other government staff concerning a competitively bid contract or a professional services procurement, the Board member shall:

a. Accept the information or inquiry and provide such information to the Board for response; or
b. Decline to discuss the information or to respond to the inquiry or complaint and instead refer the matter to the Agency Program Manager.

IV. Once a request for bids, request for qualifications or request for proposals is issued by the Agency, Agency officials are encouraged to decline meetings or informational exchanges with potential bidders or proposers. Requests for meetings or information should be referred to the Agency Program Manager.

V. If the information or an inquiry received by an Agency official indicates there may have been a violation of applicable laws, regulations, Board policies, member jurisdiction policies, or administrative procedures, the Board member should promptly refer such complaint, information, or inquiry to the Chair for response. Employees should consult with the Program Manager of the Agency. The Chair may direct the issue to the Program Manager of the Agency and/or legal counsel for response.

D. Conflicts of Interest

I. No Agency official shall engage in any act which is in conflict with the performance of his or her official duties for the Agency or knowingly use his or her office or position for personal or immediate family gain or profit.

II. Any Agency official shall be deemed to have a conflict of interest if the Agency official engages in any of the following activities:

a. Has or is seeking to advance or obtain contractual or other business or financial relationships with the Agency.

b. Conducts operations or activities regulated by the Agency.

c. Has interests which may be substantially affected by the Agency official's performance or non-performance of his or her official duties for the Agency.

d. Receives or has any financial interest in any sale or lease to the Agency of services, materials, equipment or property when such financial interest is received with the prior knowledge that the Agency intends to purchase, lease or contract for such services, materials, equipment, or property.

e. Participates in his or her capacity as an Agency official in the making of a contract in which he or she has a private pecuniary interest, direct or indirect, or performs in regard to such a contract some function requiring the exercise of discretion on behalf of the Agency.

f. Influences the Agency's selection of, or its conduct of business with, a corporation, person or firm having business with the Agency if the Agency official has financial interest in or with the corporation, person, or firm.

g. Engages in, accepts private employment from or renders services for private interests when such employment or service is incompatible with the proper discharge of official duties or would tend to impair independence of judgment or action in the performance of official duties for the Agency.

h. Appears on behalf of a private person, other than his or herself or an immediate family member or except as a witness under subpoena, before any regulatory governmental agency or court of law in an action or proceeding to which the Agency or an Agency member in an official capacity is a party or accepts a retainer or compensation that is contingent upon a specific action by the

Agency. Discloses or uses, without legal authorization, confidential information concerning the property or affairs of the Agency in such a way as to benefit himself or herself or a member of his or her immediate family with respect to any contract or transaction which is or may be the subject of official action of the Agency.

i. Has a financial or personal interest in any action or decision coming before the Agency and participates in discussion with or gives an official opinion to the Agency unless:

i. The Agency official discloses on the record of the Agency the nature and extent of such interest or makes a good faith effort to comply with the disclosure requirement and procedures included within these policies, and

ii. It is confirmed that a conflict of interest does not exist, or such interest is determined by the Agency to be immaterial.

iii. Takes any action in the course of his or her official duties for the Agency in ~~regards~~regard to providing service to specifically benefit the regulation or development of property or of a private business or enterprise in which the Agency official holds an interest in, directly or indirectly, for purposes of personal financial gain, investment or speculation provided, that this prohibition shall not apply to:

iv. Real property devoted to the personal use or residence of the Agency official or a member of the Agency official's immediate family, or

v. Any other interest in real property held by an Agency official on the date of enactment of these policies.

vi. Participates in a transaction involving the appointment, termination of appointment, promotion, demotion, discipline, approval of a salary increase or decrease or the supervision of the work of a member of their immediate family or any other person in whom the Agency official has a financial interest. The conflict of interest prohibitions of this Section shall not apply to activities between a consultant for the Agency or persons employed by or serving as subcontractors.

E. Conduct of Agency Officials

I. Agency officials will conduct themselves according to the rules of conduct below as they pertain to their public service for and on behalf of the Agency.

II. Agency officials shall maintain decorum in meetings and set an example of exemplary conduct when Agency officials represents the Agency. Agency officials shall conduct themselves so as not to bring disgrace or embarrassment upon the Agency.

III. Agency officials shall always represent that opinions stated are the Agency official's own and do not necessarily represent those of the Agency unless the Agency Board has voted and passed a resolution or motion that so states or clearly supports the expressed policy

.

IV. No Agency official shall willfully make any false statement, certificate, mark, rating, or report or in any manner commit any fraud, conceal any wrongdoing or knowingly withhold information about wrongdoing in connection with work-related conduct of any Agency official.

V. Agency officials shall devote their best efforts and attention to maintaining honest, open, and civil communications at all levels of the Agency and with the public.

5. Compliance

A. In order to ensure that the personal and financial interest of Agency officials present no actual or apparent conflicts of interest when any matter in which an Agency official has a personal or financial interest comes before the Agency Board or its standing committees for action or recommendation, the Agency official shall promptly disclose the general nature and extent of such interest on the record of the meeting prior to any discussion or vote on the matter.

B. If a conflict of interest is confirmed through the process described in the next section, the Agency official shall disqualify himself or herself from discussion or voting upon the matter, and shall refrain from discussion or recommendation concerning the matter, if discussion or voting thereon would constitute a conflict of interest, or apparent conflict of interest, as described in this section or violate any other governmental law or regulation.

C. Any Agency official who is disqualified by reason of such conflict of interest shall, after having made the required disclosure set forth above, remove himself or herself from his or her customary seat, or teleconference, during such debate and leave the Board chambers until such time as the matter at hand, from which such Agency official has been disqualified, has been disposed of in the regular course of business. Any action taken by the Board or a committee related to such interest shall be by a vote sufficient for the purpose without counting the vote of the Agency official having the interest.

D. If an Agency official is uncertain whether he or she may have an actual or apparent conflict of interest concerning any matter which is proposed for discussion, action or recommendation by the Agency Board or one of its standing committees, the Agency official shall refrain from communicating with other Board members concerning the matter unless:

I. Such conflict has been disclosed as provided above at a public hearing of the Board or a standing committee and resolved by the chair of the meeting, or

II. Legal counsel of the Agency has been advised of the basis for the questioned actual or apparent conflict and has determined that no conflict of interest as defined by this resolution exists which would either require disclosure or deferral of any discussion, action or recommendation.

E. ~~E.~~ If during the course of discussion of matters by the Board or a standing committee, a Board member concludes that his or her continued participation may constitute an actual or apparent conflict of interest which was previously unanticipated, he or she shall promptly inquire of the chair of the meeting and Agency legal counsel whether or not disclosure as provided by this section is appropriate or required and proceed as directed by the chair and legal counsel. The discovery and disclosure as provided herein of a previously unanticipated and unintended conflict of interest by a Board member or during his or her discussion of matters pending before the Board or a standing committee shall not disqualify the Board or committee from subsequently taking an action or making a recommendation.

F. ~~F.~~ If the Program Manager or an employee is uncertain whether he or she may have an actual or apparent conflict of interest they should not make a unilateral decision if there is any doubt, including his/her ability to impartially review a matter involving one's social contact, acquaintance, or friend. The Agency legal counsel should be consulted.

6. Complaints

The Executive Board shall insure the proper implementation of the code of Ethics and will investigate and report on alleged conflicts of interest. The Agency's legal counsel shall be available and shall serve as technical staff for the Board throughout the review process.

A. The Board shall meet within thirty (30) days after receipt of any written complaint.

B. The Board shall render opinions, in writing, concerning questions of ethics, conflicts of interest, and applicability of this Code of Ethics. The Board shall limit its scope to specific complaints and shall not go beyond matters relating to the complaint.

C. The Board shall investigate all formal written complaints, from any source, with regard to alleged violations of this policy if the complaint is determined to be sufficient by legal counsel. The Board may also defer investigation of the complaint to the member jurisdiction for the member who is the subject of the complaint.

D. In the course of its investigation, the Board may require any Board member or the Program Manager or request any other person to appear before the Board to give full information under oath and to produce books, memoranda, papers, documents, financial statements, receipts, canceled checks, or any other relevant information or data in the possession, custody, or control of the person ordered or requested to appear.

E. All witnesses required or requested to attend such hearings shall receive written notification, in person or by certified mail, of the time and place of the hearing at least fifteen days prior to the date fixed for attendance

F. Whenever an Agency official is under investigation for any alleged violation of this Code, he/she shall receive appropriate notice in writing from the Board at least fifteen days prior to any hearing. That Agency official shall also be entitled to be present, to examine and cross-examine witnesses, to be represented by counsel, and to call witnesses on his/her own behalf.

G. In order to protect the rights and reputation of persons who may be unjustly attacked or criticized and given the fact that investigations of complaints may serve as a prelude to further legal or disciplinary action, hearings concerning violations of this Code shall be conducted in private to the extent permitted by state law; provided that, the person subject to the complaint may request that the hearings be conducted in public. A record of such proceeding shall, however, be made and retained.

H. Provided, however, that any Agency official who is the subject of a complaint may demand a public hearing. All hearings whether public or private shall be conducted under the guidelines established herein.

I. The Board shall render a written record of its findings upon conclusion of the investigation.

J. The record of the Board's written findings shall be open to public inspection unless:

i. The information is exempt according to state law (RCW 42.56) and damage to individuals resulting from the release of the record would outweigh the public's need to know;

ii. The Board has determined in the conduct of any hearing or proceeding under its jurisdiction that it is reasonable to withhold information in order to protect individuals who may be unjustly or improperly accused or who may be disproportionately harmed or injured in their reputation, employment, or profession by any premature disclosure;

iii. Civil or criminal action by the Agency or any other governmental agency having jurisdiction may be pending.

7. Remedy

A. If a board member is found to be in violation with these policies, the board may send a letter of admonishment to the member jurisdiction and seek a remedy in accordance with the Agency by-laws.

B. If the Program Manager is found to be in violation he or she will be subject to disciplinary action up to and including termination from employment; provided that, in the event that the Program Manager is a loaned employee, any disciplinary action shall be subject to and implemented in accordance with any agreements in place between the Agency and the employer of the Program Manager.

C. In the event the Board's findings disclose an apparent violation of any state law, a copy of the findings shall be filed with the Prosecuting Attorney of King County.

D. If the Board's findings disclose an apparent violation of any local law, then the Agency's legal counsel may prosecute by appropriate action of either a criminal or civil nature.

E. Any sufficient complaints regarding Agency employees shall be referred to the Program Manager of the Agency, who shall investigate the complaint and take appropriate action

Emergency Procedures

1. Purpose

To clarify roles and responsibilities in the event of an emergency.

2. Policy

A. FileLocal staff shall follow City of Seattle emergency procedures during the term of the Agreement between FileLocal and the City of Seattle for using City of Seattle office space.

B. Security procedures and roles and responsibilities during an emergency related to the tax portal are described in the service provider agreement between the City of Seattle and e-Gov. These procedures will be reviewed by the Executive Board and will require Executive Board approval. Following approval, the security procedures will be appended to the operating procedures.

C. FileLocal shall have a management group responsible for contingency plans including a line of succession.

3. Responsibility

Program Manager

4. Procedure

A. The Program Manager shall brief the Executive Board on all emergency plans included within the City of Seattle emergency procedures, tax portal service agreement, and communications policies.

B. The Agreement between FileLocal and the City of Seattle provides that the City may backfill a support staff member for a period of less than three consecutive weeks.

C. The line of succession for the Program Manager is as follows: Information Technology Business Analyst (Project Manager).

~~C.~~ The Executive Board shall establish a line of succession in the event of an emergency that affects personnel in the City of Seattle including the Program Manager and the City of Seattle's Board Member. This succession is as follows: Executive Board Chair; Executive Board Vice-Chair; remaining Executive Board member(s).



FISCAL MANUAL

December 2019



Fiscal Manual

TABLE OF CONTENTS

Internal Control 2
Accounting Systems 3
Budget 4
Cash Management 5
Cash Receipts and Deposits 6
Local Government Investment Pool 7
Disbursements ..... ~~7~~8
Revenue and Receivables ..... ~~14~~15
Procurement and Contract Management ..... ~~16~~17
Capital Asset Management ..... ~~18~~19
Journal Entries 21
Financial Reporting 22
Financial Forms 23

1. Internal Control

1.1 Purpose

To ensure that FileLocal assets are received when tendered, protected while in custody, and used only for the purposes intended. To segregate duties and responsibilities so that one person does not handle all phases of a transaction. To establish policies and procedures so that errors, omissions, and irregularities are detected and minimized.

1.2 Policy

Policies and procedures established for the accounting functions shall be designed to achieve and preserve, to the maximum practical extent, internal controls to safeguard the assets of FileLocal, minimize and detect errors and omissions, and maintain an audit trail for independent review of FileLocal's activities.

1.3 Responsibility

Executive Board, Program Manager, the Agency's accounting firm and Others

1.4 Procedure

A. Financial statements and related supporting work prepared by the Agency's accounting staff on behalf of FileLocal shall be reviewed by senior level staff within the Agency's accounting firm.

B. Financial statements prepared by the Agency's accounting firm shall be reviewed by FileLocal's Program Manager on a monthly basis.

C. The Program Manager and Executive Board review, per the resolution authorizing the FileLocal Executive Board meetings for the year, the financial reports, budget variance, and large or unusual transactions.

D. Accounting documents and records shall be maintained in safe, secured drawers and network server at the Agency's accounting firm to prevent their inadvertent or intentional loss.

E. Although not designed exclusively to catch fraud, should our internal control procedures uncover fraud, the Program Manager, the Executive Board, and the State Auditor will be notified within 5 business days.

~~10.~~2. ~~2.~~ Accounting Systems

2.1 Purpose

To describe the fundamental system for accounting, the internal controls within the financial operation, and the reconciliation between functional areas.

2.2 Policy

Automated and manual accounting systems shall be maintained and reconciled to provide a comprehensive and consistent accounting reporting system that meets federal, state, and local requirements, as well as generally accepted accounting principles.

2.3 Responsibility

The Agency's accounting firm shall establish and maintain a system that ensures that both integrated and independent accounting modules reconcile to the general ledger of FileLocal, and that proper internal controls exist within the various systems to protect the integrity of the data, safeguard the assets of FileLocal, and identify errors and irregularities in the normal course of financial operation.

2.4 Procedure

A. The automated accounting system QuickBooks consists of three components that integrate to produce accurate financial reports and other pertinent information related to the accounting process:

   I. General Ledger

   II. Accounts Receivable

   III. Accounts Payable

B. Capital assets, prepaid expenses and long-term assets and liabilities that are depreciable and amortizable are maintained in Excel spreadsheets. These are designed for FileLocal to keep detailed information to meet the accounting needs of the Agency. Manual systems are reconciled to QuickBooks on a monthly basis.

C. Backup of QuickBooks is performed periodically, at least once a year.. All essential worksheets and other files that are maintained by the Agency's accounting firm are stored on its network server and backed up daily. Records and files are retained at the Agency's accounting firm for seven (7) years.

~~11.~~3. Budget

3.1 Purpose

The biennial budget and related processes provide a tool for achieving financial oversight over the FileLocal's financial well-being. In addition, the budget enables the Program Manager and Executive Board to focus on anticipated revenue, estimated expenditures, capital asset acquisition, long term financial health, and continuity of services.

3.2 Policy

On an annual basis, the Agency will develop and propose a budget for revenue and expenditures for overall program and administration. The budget will be developed, adopted, and administered in accordance with Section 13 of the Interlocal Agreement.

3.3 Responsibility

Executive Board, Program Manager, and the Agency's accounting firm

3.4 Procedure

A. On an annual basis, the Program Manager and the Agency's accounting firm will draft initial revenue and expenditure forecasts. During the annual budget process, the needs of FileLocal are evaluated to ensure proper staffing to meet the needs of the consortium, ensure website data security, and meet the organizational goals. This budget is - in part - established based on the number of customers and emerging community needs.

   a. Reimbursement Allocation: Costs will be allocated to Original Principals and new Participating Cities as follows:

      i. Original Principals – Bellevue, Everett, Tacoma, and Seattle. Allocation will be done using the 2012 actual historical transaction counts through FY 2021. After 2021, the reimbursement allocation will be based on actual transactions processed on the Portal.

      ii. New Participating Cities – The cities' historical counts agreed on during the implementation phase will be used through FY 2021. After 2021, the reimbursement allocation will be based on actual transactions processed on the Portal.

B. The proposed budget is submitted to the Operations Committee for preliminary review and to the Executive Board for its final review and ultimate approval of the budget.

C. Modifications to the budget shall be approved by a supermajority vote of the Executive Board (and also unanimous consent of the Original Principals if required by Section ~~13b~~13 b.iv of the Interlocal Agreement) as necessary from time to time to account for changes in expenditures and revenues.

D. The budget is monitored through a monthly schedule of actual and budget comparisons submitted by the Agency's accounting firm. This schedule shows the variances between year-to-date revenue and expenditures, and amounts budgeted by the Agency.

~~12.~~4. Cash Management

4.1 PURPOSE

To outline the policy for cash management.

4.2 POLICY

FileLocal shall maintain an effective system of cash management that anticipates cash needs and have plans to meet its cash flow needs.

4.3 RESPONSIBILITY

Program Manager and the Agency's accounting firm

4.4 PROCEDURE

A. All receipts shall be deposited within 3 business days.

B. Disbursements shall be released within 30 days, no later than due date.

C. Every effort will be made to take advantage of early pay discounts if they result in benefit to FileLocal.

D. The Agency's accounting firm shall maintain a current daily balance of checking accounts and shall record deposits and checks in such manner to know the available cash balances at all times.

E. Bank reconciliation is performed by the Agency's accounting firm on a monthly basis and subject to review by the Program Manager.

F. The operating cash reserve goal is to maintain a reserve equal to 15% of the annual budget, consistent with the reserve fund provision in section 13 m. of the Interlocal Agreement.

G. Excess cash shall be invested into the Local Government Investment Pool (LGIP).

~~13.~~5. Cash Receipts and Deposits

5.1 PURPOSE

To outline cash receipts and deposit policies and procedures.

5.2 POLICY

All fees, receipts, and income collected or received are deposited into FileLocal's bank depository account.

5.3 RESPONSIBILITY

Program Manager and the Agency's accounting firm

5.4 PROCEDURE

A. Cash receipts received by mail at FileLocal Office shall be forwarded to the Agency's accounting firm within 3 business days. Cash receipts received by mail at the Agency's accounting firm are deposited into FileLocal's bank account at Wells Fargo within 3 business days. Checks received must be safekept in a secured drawer.

B. The Agency's accounting firm Administrator opens, sorts, and deposits cash receipts. Deposit slips and copies of checks are given to an accountant at the Agency's accounting firm for booking cash receipts in FileLocal's accounting system.

C. Service fees collected or received by the third-party service company are electronically swiped/transferred to FileLocal's bank account at Wells Fargo. The third-party service company shall provide the Agency's accounting firm daily cash receipts data and documents on a monthly basis.

D. Cash receipt data and documents submitted by the third-party service company are reconciled by the Agency's accounting firm and entered in FileLocal's accounting system. If any errors are encountered, the Agency's accounting firm will notify both the Program Manager and the third-party service company of any overage or shortage. the Agency's accounting firm will contact the third-party service company to obtain the necessary information to make the correction. Once the receipt is correct, the Agency's accounting firm will update the FileLocal general ledger and communicate the corrected data to the Program Manager.

E. Cash receipts are reconciled to bank statements by the Agency's accounting firm on a monthly basis. Monthly bank reconciliation shall be reviewed by the Program Manager.

5.4.1 Local Government Investment Pool

1. Purpose

To outline local government investment pool policies and procedures.

2. Policy

Excess cash shall be invested to the local government investment pool (LGIP). For the purpose of determining the excess cash, excess cash shall be any amount that exceeds $250,000 at the end of the month.

3. Responsibility

Executive Board, Program Manager, and the Agency's accounting firm

4. Procedure

A. The Agency's accounting firm calculates the excess cash on a monthly basis for the purpose of the LGIP investment. The calculation is reviewed by the Program Manager.

B. After any contribution or withdrawal are reviewed and approved by the Program Manager, the Agency's accounting firm follows the LGIP Operation Manual to process the transaction. The minimum contribution or withdrawal shall be $5,000. The minimum amount is required by the LGIP in accordance with WAC 210-01-060.

C. The LGIP paperwork, such as Local Government Investment Pool Authorization Form and TM$ Online Web Access shall be completed by the Program Manager or Treasurer (CEO of the Agency's accounting firm). According to the Resolution No. FL2020-02, the Program Manager and Treasurer are the authorized individuals to authorize all amendments, changes, or alternations to the LGIP documents.

D. The Agency's accounting firm receives the monthly LGIP statement. The Agency's accounting firm conducts a monthly reconciliation. The Program Manager reviews the monthly reconciliation.

E. On a quarterly basis, the Program Manager will present the LGIP activities to the Executive Board for the Board's review.

~~14.~~6. Disbursements

6.1 ~~6.1~~ AUTHORIZATIONS

1. PURPOSE

To establish signature approval levels for the purpose of authorizing purchases, contracts, and expenditures.

2. POLICY

Authorizations for purchases, contracts and all other expenditures excluding the purchase requests made by the Program Manager must follow this delegation of authority

- Unbudgeted authorizations < $5,000 must be approved by the Executive Board Chair and Vice-Chair.
- Unbudgeted authorizations > $5,000 must be approved via a resolution with the Executive Board
- Budgeted authorization < $50,000 must be approved by the Program Manager
- Budgeted authorization > $50,000 must be approved by the Executive Board Chair and Vice-Chair
- All contracts in excess of $5,000 shall be briefed and reviewed with the FileLocal Executive Board at regularly scheduled Executive Board Meeting prior to authorization.

Authorizations for purchases, contracts and all other expenditures requested by the Program Manager must follow this delegation of authority.

- Unbudgeted authorizations < $2,000 must be approved by the Executive Board Chair and Vice-Chair.
- Unbudgeted authorizations > $2,000 must be approved via a resolution with the Executive Board
- Budgeted authorized < $5,000 must be approved by the Treasurer
- Budgeted authorized > $5,000 must be approved by the Treasurer and either the Executive Board Chair or Vice-Chair.
- All contracts in excess of $5,000 must be briefed and reviewed with the FileLocal Executive Board at regularly scheduled Executive Board Meeting prior to authorization.

3. RESPONSIBILITY

The Program Manager, Executive Board, and the Agency's accounting firm.

4. PROCEDURE

Prior to purchase and/or disbursement all applicable forms and paperwork, including but not limited to Purchase Acquisition Form, must be authorized in accordance with the above policy. See Attachment A for Purchase Acquisition Form.

6.2 Cash Disbursements

1. Purpose

To outline the policy for cash disbursements.

2. Policy

Disbursements shall be made only for valid transactions by authorized personnel only.

3. Responsibility

The Program Manager, Executive Board, and the Agency's accounting firm

4. Procedure

A. All disbursements and electronic fund transfers, including ACH transactions, shall be for FileLocal business and each transaction must be supported with properly authorized documentation such as an invoice, payroll record, or expenditure/check request.

B. Invoices and requests for payment must be reviewed and approved by the Program Manager before checks are prepared. Prior to payment, the Agency's accounting firm verifies the authorization of purchase, expenditures, and invoices. A Payment Approval Checklist shall be filled out. See Attachment B for Payment Approval Checklist.

C. The Agency's accounting firm prepares checks and also maintains and initiates electronic payments. Maintenance of vendor information files and initiating of payments will be performed by two separate staff persons at the Agency's accounting firm.

D. Checks made payable to "bearer" or "cash" or signed blank are prohibited.

E. Checks are mailed directly to the payee by the Agency's accounting firm.

F. Checks or electronic payments that are returned or rejected must be investigated and resolved within 2 business days of receipt/notification in order to avert loss from fraud or negligence.

G. Bank statements are received in the mail, reviewed, and reconciled to the general ledger on a monthly basis by the Agency's accounting firm. Copies of checks are to be matched to the supporting documentation. Prior to filing, all disbursement support shall be reviewed for proper documentation and approving signatures. Bank reconciliations and cancelled checks will be available for review by the Program Manager.

A list of vendor names and disbursements is prepared by the Agency's accounting firm and sent to the Executive Board for review on a quarterly basis.

6.3 Check Request

1. Purpose

To outline the policy for check requests.

2. Policy

The Check Request form (see attachment C) must be completed for all expenditures not covered by a Purchase Order Requisition or detailed invoice.

3. Responsibility

The Program Manager shall be responsible for signing check requests to indicate approval. Check and reimbursement request must follow the Authorization Policy in 6.1.2 A&B.

4. Policy Exceptions

A recurring payment does not require a Check Request for the Executive Board or the Program Manager's authorization. These expenditures have been constructively approved by virtue of the Executive Board's approval of the contracts and agreements giving rise to the recurring obligation. A sample list of these types of expenditures is as follows:

A. Purchase orders supported by purchase requisitions;

B. Contract payments supported by previously approved contracts;

C. Pre-authorized temporary personnel help;

D. Contracted labor costs and allocated overhead..

5. Procedures

For the items listed below, no Purchase Order Requisition form is required. A Check Request form may be used: The approval thresholds follow 6.1 Authorizations.

A. US Postal costs;

B. Licenses;

C. Conference fees, tuition, and temporary employment services;

D. Freight bills, express shipping, common carriers, import/export duties, customs & brokerage fees;

E. Travel expenses, including transportation, meals, and hotel;

F. Dues, subscriptions, professional membership & association dues, and

G. Advertising.

6.4 Check Control

1. Purpose

To detail the policy and procedures for control of signed checks and unsigned check stock.

2. Policy

All checks are to be accounted for by check number. the Agency's accounting firm shall maintain internal controls with respect to custody of check stock, preparation, printing, signing, mailing, filing, and voiding of all checks.

3. Responsibility

The Agency's accounting firm

4. Procedure

A. Check stock is to be securely maintained in a locked cabinet at the Agency's accounting firm.

B. the Agency's accounting firm is responsible for typing or printing checks after verifying the approval of payments..

C. Bank reconciliation will include accounting for all void or destroyed checks.

D. All checks will be signed by the authorized check signers – the Program Manager or the Treasurer.

Cancelled checks with bank reconciliation and bank statement prepared by the Agency's accounting firm are forwarded to the Program Manager for review on a monthly basis.

6.5 Travel Expense

1. PURPOSE

To outline the policy for travel expense reimbursement and ensure adequate cost controls are in place, travel expenditures are appropriate and provide a uniform and consistent approach for timely reimbursement of authorized expenses. For the purpose of this policy, Board members are considered staff.

2. POLICY

It is the policy of FileLocal to reimburse staff for reasonable and necessary expenses incurred in connection with approved travel on behalf of FileLocal. FileLocal strongly encourages use of travel discounts when making travel arrangements.

Travelers seeking reimbursement should incur the lowest reasonable travel expenses and exercise care to avoid impropriety or the appearance of impropriety. Reimbursement is only allowed when not available or provided by other sources. If a circumstance arises that is not specifically covered in this travel policy, then the most conservative course of action should be taken.

3. RESPONSIBILITY

Staff travel must be authorized prior to expenditures being incurred. Travelers should verify that planned travel is eligible for reimbursement before making travel arrangements. Within 30 days of completion of a trip, the traveler must submit a check request form and supporting documentation to obtain reimbursement of expenses. The authorization and check requests must follow the same process as outlined in 6.1 Authorizations and 6.3 Check Requests.

4. PROCEDURE

A. Authorized business travel for staff must be pre-approved.

B. Conference registration fees can be pre-paid with a check prepared by the Agency's accounting firm with a completed and approved check request form.

C. Requests for reimbursements of travel-related expenses are submitted via a check request form. This form must be accompanied by supporting documentation and is required to be approved by the Program Manager. Reimbursement requests for the Program Manager must be approved in accordance with ~~6.1~~61. Authorizations.

D. The check request form must be submitted to the Agency's accounting firm within 14 calendar days after the trip is completed. Exception approval from the Program Manager or Treasurer is required if this form is not submitted within this timeframe.

E. Reimbursement of travel expenses is based on documentation of reasonable and actual expenses supported by the original itemized receipts. Reimbursements that may be paid by FileLocal are shown below:

Airfare: An original itemized airline receipt, an e-ticket receipt/statement or an Internet receipt/statement is required. The receipt must show the method of payment and indicate that payment was made. Travelers are expected to obtain the lowest available airfare that reasonably meets business travel needs. Travelers are encouraged to book flights at least 20 days in advance to avoid premium pricing. Coach class or economy tickets must be purchased for domestic or international flights. A higher-priced coach ticket cannot be purchased for a subsequent upgrade in seating. First-class tickets are not reimbursable.

Rail Transportation: FileLocal will pay for rail transportation provided the cost does not exceed the cost of the least expensive airfare. An original itemized receipt, original e-ticket receipt/statement or Internet receipt/statement is required. The receipt must show the method of payment and indicate that payment was made.

Automobile (personally owned): A valid driver's license issued within the United States and personal automobile insurance are required for expenses to be reimbursed. Drivers should be aware of the extent of coverage (if any) provided by his or her automobile insurance company for travel that is business or not personal in nature. Reimbursement for use of a personal automobile is based on the mileage rate issued by the Internal Revenue Service. Travelers may opt to request reimbursement for gasoline in lieu of the mileage. In these instances, original itemized receipts are required. A check request form is required for reimbursement for all vehicle-related expenses.

Automobile (rental): Reimbursement for a commercial rental vehicle as a primary mode of transportation is authorized only if the rental vehicle is more economical than any other type of public transportation, or if the destination is not otherwise accessible. Vehicle rental at a destination city is reimbursable. Original receipts are required. When vehicle rentals are necessary, FileLocal encourages travelers to purchase collision damage waiver (CDW) and loss damage waiver (LDW) coverage. FileLocal will reimburse the cost of CDW and LDW coverage; all other insurance reimbursements will be denied. Travelers are required to fill the gas tank before returning the vehicle to the rental agency to avoid service fees and more expensive fuel rates.

Conference Registration Fees: If the conference fee was not prepaid, FileLocal will reimburse these fees, including business-related banquets or meals that are part of the conference registration. Original receipts to support the payment are required. If the conference does not provide a receipt, then a cancelled check, credit card slips/statement or documentation that the amount was paid is required for reimbursement.

Lodging (commercial): The cost of overnight lodging will be reimbursed to the traveler if the authorized travel is 45 miles or more from the traveler's home or primary worksite. The Runzheimer Cost Index will be used for determining the maximum allowable expense for all lodging at the travel destination, with the following exceptions:

a. When the hotel or motel is the conference or convention site, the conference rate is allowable.

b. When the event sponsor arranges the lodging for the event participant, the participant rate is allowable. If the hotel where the event is scheduled in unavailable to the employee, the employee's supervisor may approve lodging expenses at the rate charged at the nearest hotel.

c. Allowable lodging expenses include the cost of lodging and any applicable sales taxes and/or hotel/motel taxes. The original, detailed lodging receipt must be submitted with the expense claim.

d. If reserved rooms are not needed, it is the traveling employee's responsibility to make sure the room is canceled.

Meal: FileLocal will pay a per diem amount for meals based on the Runzheimer Cost Index for meals by location. These meal per diem amounts include tips.

a. The amount of authorized meal allowance is determined on a per meal basis dependent upon the departure time from Seattle and the arrival time on return to Seattle. Snacks and/or meals served on the airlines will not reduce the meal allowance.

b. If meals are included in a lodging, conference or training registration fee, the employee's daily per diem will be adjusted accordingly. A "continental" breakfast provided at a meeting, conference or training session will not reduce the employee's meal allowance.

c. Reimbursement of meal expenses will be based on actual expenses per meal, limited to the allowable maximum established by the Runzheimer Cost Index. Employees are required to collect original meal receipts for all allowable expenses incurred and to submit those receipts with their expense report.

Parking: Original receipts are required for parking fees, including airport parking. The lodging bill can be used as a receipt when charges are included as part of the overnight stay.

Other Travel Expenses: Other travel expenses, including faxes, photocopies, internet charges, data ports and business telephone calls incurred while traveling, can be reimbursed. Original itemized receipts are required.

The following items that may be associated with business travel will not be reimbursed by FileLocal:

a. Airline club membership

b. Airline upgrades

c. Business class for domestic flights or first class for all flights

d. Childcare, babysitting, house-sitting, or pet-sitting/kennel charges

e. Commuting between home and the primary work location

f. Costs incurred by traveler's failure to cancel travel or hotel reservations in a timely fashion

g. Evening or formal wear expenses

h. Haircuts and personal grooming

i. Laundry and dry cleaning

j. Personal entertainment expenses, including in-flight movies, headsets, health club facilities, hotel pay-per-view movies, in-theater movies, social activities, and related incidental costs

k. Travel accident insurance premiums or purchase of additional travel insurance

l. Other expenses nor directly related to the business travel

~~15.~~7. Revenue and Receivables

7.1 Revenue Recognition

1. Purpose

To establish revenue recognition policy and procedures.

2. Policy

All revenue is recognized in accordance with generally accepted accounting principles.

3. Responsibility

Executive Board, Program Manager, and the Agency's accounting firm

4. Procedure

A. Current revenue consists of service fees, reimbursable costs, and shared cost reimbursement from participating cities of FileLocal.

B. Service fees are recognized at the time a customer completes his or her licensing application. Cash basis might be used for the monthly financial reporting; however, service fees would be accrued under GAAP (generally accepted accounting principles) on the annual financial statements.

C. Reimbursable costs are pre-determined through budget, subscriber agreement or inter-local agreement, including any amendments. Reimbursable costs are billed at the beginning of the year and recognized as revenue at that time. On an annual basis, actual costs to be reimbursed are compared to amounts budgeted and billed. Adjustments will be made to reconcile billed reimbursable costs to accrual amount of costs incurred. Credits might be issued to the participating cities when an overbilled amount is identified; and as a result, a reduction of revenue is recognized. If additional costs are identified to be reimbursed from the participating cities, additional invoices are submitted to the participating cities. Additional reimbursable costs are also recognized when billed.

D. For cities which join FileLocal during the year, the reimbursable costs will be billed based on the go live date.

E. Any other contributions and donations are recognized as revenue when cash is received.

F. Any changes in revenue recognition shall be made in writing by the Program Manager and/or the Agency's accounting firm and is subject to approval by the Executive Board.

7.2 Billings and Accounts Receivable

1. Purpose

To ensure billings are made for services actually provided and based on the Interlocal Agreement, subscriber agreement or budget.

2. Policy

FileLocal shall follow prudent and efficient business practices to obtain payment of its receivables.

3. Responsibility

Executive Board, Program Manager, and the Agency's accounting firm

4. Procedure

A. Service fees are paid by customers when they submit their licensing applications. Automatic billing and payment processing are done daily by the third-party service company. the Agency's accounting firm performs a monthly reconciliation of service fees and cash receipts. The monthly reconciliation is forwarded to the Program Manager for review.

B. the Agency's accounting firm prepares invoices for reimbursable cost revenue based on the budgeted amount established at the beginning of the year and/or the prorate share of new cities. At year-end, the Agency's accounting firm conducts a reconciliation of reimbursables according to the actual operation revenue. Any refund or under-billed amounts identified by the Agency's accounting firm through the annual reconciliation is subject to review and approval by the Program Manager and then the Executive Board. Refunds or additional invoices are then processed by the Agency's accounting firm.

C. On a monthly basis, Accounts Receivable is reconciled by the Agency's accounting firm. For any delinquent balance, the Agency's accounting firm sends letters requesting payment and makes a reasonable effort via other means to contact and collect outstanding balances. Monthly Accounts Receivable aging reporting is included in the monthly financial statement packet for the Program Manager and the Executive Board's review.

D. Any adjustments and write-off to Accounts Receivable (excluding purely accounting adjustments/corrections) is subject to approval by the Program Manager. Any the write-off amount in excess of $2,000 is also subject to approval by the Executive Board.

E. All payments received by the Agency's accounting firm are reconciled to Accounts Receivable, the general ledger, and the bank deposits (part of monthly bank reconciliation).

~~16.~~8. Procurement and Contract Management

8.1 Procurement

1. Purpose

To outline procurement policies and processes.

2. Policy

All contracts for labor, professional services, lease of equipment, and supplies for $10,000 or more must be let by free and open competitive bidding, on sealed bids, to the responsible bidder.

3. Responsibility

Executive Board and Program Manager

4. Procedure

A. FileLocal is required to advertise for sealed bids on contracts for labor, professional services, and equipment leases in excess of $10,000 by posting a notice at its website or by publication of a one-time notice in a newspaper published in the State of Washington.

B. In case of an emergency affecting the public's health, safety, economic welfare, or security, a contract may be let to the extent necessary to meet the emergency without public advertisement. The Program Manager will honor payment for a period of six months from the date of declaration posting; should the emergency continue to exist after a six-month period, it will be necessary to re-declare the emergency.

C. Sealed bids are accepted by the Program Manager for evaluation. Based on the Program Manager's recommendation, the Executive Board approves and awards the responsible bidder through competitive bidding with consideration given for the quality of the commodities, conformity to specifications, terms of delivery, and freight charges. Multiple awards may be issued, if notice is contained within the competitive bid, when technical compatibility and/or operational specification are required.

D. A contract for labor, professional services and equipment leases will be let for periods no greater than five years.

E. An awarded contract is not assignable by the bidder without written consent of FileLocal. A contract cannot be assigned to a bidder whose bid was rejected.

8.2 CONTRACTS

1. PURPOSE

To provide policy and procedures for the review, approval, establishment, and modification of personal and professional services contract.

2. POLICY

All contracts should be authorized according to the Authorization Policy and approved as to form by the Agency's attorney.

3. RESPONSIBILITY

Executive Board and Program Manager

4. PROCEDURE

A. Personal and professional service contracts must include the following information:

   I. Name, including contract name and tax identification number (Form W-9);

   II. Scope of contract – what is to be done, the purpose, goal, job, etc.;

   III. Term of contract, including the beginning and ending dates;

   IV. Total contract amount and the method of payment;

   V. Termination clause;

   VI. Signatures.

B. A contract cannot be assigned to a third party. If a different contractor is required, the original contract must be canceled, and a new contact must be initiated.

C. An emergency contract for personal or professional services shall be let for a period of not more than 6 months.

D. Contracts between governmental entities must be separately tracked to ensure additional reporting and regulatory compliance required by federal and state law.

~~17.~~9. Capital Asset Management

9.1 Capitalization Policy

1. Purpose

To define capitalization policy.

2. Policy

All personal and real property with an initial individual cost of more than $5,000 and an estimated useful life in excess of two years are recognized as capital assets. Such assets are recorded at historical cost. Donated capital assets are recorded at acquisition value at the date of donation. Costs for additions or improvements to capital assets are capitalized when they increase the effectiveness or efficiency of the assets. The costs for normal maintenance and repairs are not capitalized. Capital assets are depreciated using the straight-line method over the following estimated useful lives:

- Software 3 – 5 years
- Computers and equipment 3 – 7 years

3. Responsibility

Program Manager and the Agency's accounting firm

4. Procedure

A. The Agency's accounting firm shall assign the appropriate accounting classification codes to all purchases, contracts and acquisitions that qualify as capital assets.

B. The Program Manager shall provide the Agency's accounting firm copies of all purchase orders, requisitions, and receiver's reports covering capital asset purchases.

C. The Agency's accounting firm shall be responsible for recording the asset on the capital asset schedule, a manual spreadsheet/sub-ledger, showing the description, physical location, owners, cost, acquisition date, useful life, depreciation, and disposition date including the date of disposal and sales price of the property.

9.2 Physical Inventory

1. Purpose

To establish physical inventory of capital assets

2. Policy

All capital assets should be inventoried periodically, but not less than every two years, to reconcile the total capital assets with the capital asset schedule (a sub-ledger).

3. Responsibility

Program Manager and the Agency's accounting firm

4. PROCEDURE

A. The Agency's accounting firm shall perform a physical inventory of capital assets at least once every two years.

B. Once the physical inventory is complete, it must be reconciled to the individual capital asset record (a manual capital asset sub-ledger) and general ledger.

C. Inventory count sheet and reconciliation is subject to the Program Manager's review. Any discrepancy is investigated by the Program Manager.

9.3 DISPOSITION

1. PURPOSE

To outline disposition of capital assets.

2. POLICY

All capital asset dispositions shall be approved by the Program Manager. Any disposition in excess of $10,000 shall be approved by the Executive Board.

3. RESPONSIBILITY

Program Manager and the Agency's accounting firm

4. PROCEDURE

A. Disposition of capital assets shall be requested in writing and addressed to the Program Manager. Any disposition in excess of $10,000 shall be approved by the Executive Board.

B. All disposition documents shall be forwarded to the Agency's accounting firm to record the disposition. Gains and losses are recognized on the sale of capital assets.

C. The capital assets and related depreciation shall be removed from both the capital asset sub-ledger and general ledger.

9.4 CAPITAL ASSET IMPAIRMENT

1. PURPOSE

To outline capital asset impairment policy and procedures.

2. POLICY

Capital asset impairment is conducted on an annual basis or at the time the impairment occurs. Only permanent impairments of capital assets should be recognized in the financial statements.

3. RESPONSIBILITY

Program Manager and the Agency's accounting firm

4. PROCEDURE

A. The Agency's accounting firm shall conduct an impairment analysis on an annual basis, or at time the impairment occurs in accordance with the generally accepted accounting principles.

B. A memo of impairment analysis with calculated loss prepared by the Agency's accounting firm is submitted to the Program Manager for review and approval.

C. The Agency's accounting firm records impairment losses in FileLocal general ledger system.

~~18.~~10. Journal Entries

1. PURPOSE

To outline types of journal entries and internal controls over journal entries.

2. POLICY

All journal entries must be self-balancing and include an account type (asset, liability, revenue, expense, net assets) for each line of the journal entry. Journal entries are subject to review and approval based on the policies and procedures herein.

3. RESPONSIBILITY

Program Manager and the Agency's accounting firm

4. PROCEDURE

Journal entries are used to:

A. Correct errors: most of journal entries will be to correct account-coding errors. The journal entry must include the debit entries and credit entries to correctly produce the required accounting effects. There is no review or approval required for this type of journal entry prior to or after posting the journal entries.

B. Record cost allocation: cost allocation is processed by the Agency's accounting firm based on the approved cost allocation documents, including budgets. No review or approval is required for this type of journal entry.

C. Record recurring balance sheet transactions: recurring journal entries include monthly depreciation, amortization, receivable, and accrued liabilities. They are not required for review or approval.

D. Journal entries for month-end and year-end closing, such as accruals, are subject to internal controls within the Agency's accounting firm following GAAP. There is no review or approval required prior to or after posting the journal entries.

E. Implement accounting policies and guidance: a memo is prepared for the implementation of a new accounting standard by the Agency's accounting firm to the Program Manager for review and approval. The memo will provide a reference of the new accounting standard, accounting effects, and a proposed journal entry

F. Record non-routine, nonrecurring transactions: a memo in writing to the Program Manager is required for review and approval of non-routine, non-recurring transactions.

~~19.~~11. Financial Reporting

1. PURPOSE

To establish and catalog the reporting requirements for accounting.

2. POLICY

Financial statements and reports shall be prepared on a monthly and annual basis to provide the Program Manager and Executive Board, and outside auditors with sufficient financial information to report accurately the results of operations.

3. RESPONSIBILITY

The Agency's accounting firm shall maintain supporting records in sufficient detail to prepare financial statements or reports for FileLocal.

4. PROCEDURE

A. On an annual basis, Francis and Company prepares and presents:

I. Annual financial statements with full footnote disclosures,

II. Other required supplemental schedules and information.

The annual financial statements are prepared in accordance with generally accepted accounting principles. The annual financial statements along with required supplemental information are subject to review by the Executive Board and the Program Manager. The Executive Board adopts the annual financial statements.

B. On a quarterly basis, the Agency's accounting firm submits to the Executive Board to adopt:

I. List of vendor warrants.

C. On a monthly basis, the Agency's accounting firm prepares and presents:

I. Internal financial statements (currently using cash basis).

II. Schedule of actual and budget comparison.

III. Variance analysis, as needed, will be prepared with monthly financial statements.

Attachment A Purchase Requisition Form

FileLocal

Purchase Acquisition Form

Requested by:		Date:	
Purpose or Use:			
Vendor Name:			
Vendor Address:			
Vendor Contact:		Phone:	

Product/Service Description	Qty	Unit Price	Extended Cost
Approvals:		Date:	
Approvals:		Date:	

Attachment B Payment Approval Checklist

FileLocal

Payment Approval Checklist

We are required to fill out this payment approval checklist prior to processing a check payment for FileLocal. A check must be processed once the proper approval is verified through this checklist. Once this checklist is filled out and a check is processed, this checklist shall be forward to FileLocal for record.

	YES	NO	N/A
Is Purchase Acquisition Form or Check Request Form attached to an invoice/itemized receipt for processing payment? (Please Note Purchase Acquisition Form or Check Request Form is not required for a recurring payment.)			
Is Purchase Acquisition Form or Check Request Form approved by authorized person (s) in accordance with 6.1 Authorizations of Fiscal Manual? For a recurring payment, is vendor's invoice/itemized receipt approved in accordance with 6.1 Authorization of Fiscal Manual?			
Is vendor's invoice reviewed for GL coding and recording?			

Preparer:	
Date:	

Attachment C: Check Request Form

FileLocal
Check Request Form

Deliver Check to:

Date Required	Check Amount

Purpose of Payment

G/L Account #:

Vendor Name	Invoice/Receipt Number	Invoice Date	Amount

Originator	Date

Approval	Date



Information Technology Securities Policy Manual

TABLE OF CONTENTS

POL-001: Information Management 2

POL-010: Information Classification 6

POL-015: Personnel Security 9

POL-020: Access Control 11

POL-030: Encryption 14

POL-040: Infrastructure 16

POL-050: Physical and Environmental 19

POL-060: Third Party Management and Outsourced Services 21

POL-070: Data Backup 24

POL-080: Data Storage Media Library Management 27

POL-090: Compliance 30

POL-100: Incident Response 34

POL-110: Security Risk Assessment 37

POL-130: System Development Life Cycle 39

POL-140: Business Continuity 41

GDE-200: Guidelines for Information Owners and Custodians 43

Information Management

1. Purpose

The Information Management Policy defines the principles to be used in the protection of the agency's assets from all threats, whether deliberate or accidental, with the objective of ensuring business continuity, protecting employees and participating cities and minimizing the impact of security breaches.

The purpose of this policy is to:

A. Create an environment within the Washington Multi-City Business License and Tax Portal Agency (dba FileLocal) that protects the confidentiality, integrity and availability of information:

- Confidentiality: ensuring that information is accessible only to those authorized to have access
- Integrity: safeguarding the accuracy and completeness of information and processing methods
- Availability: ensuring that authorized users have access to information and associated assets when required

B. Set a uniform framework of policies by establishing principles that are to be applied throughout FileLocal in the management of information.

C. Support the selection of physical, technical and administrative security controls, which are cost- effective, prudent and operationally efficient.

D. Support the oversight functions necessary to ensure compliance with external security requirements.

E. Inform staff, vendors and participating cities of their accountability for protecting FileLocal information resources.

F. Ensure the vendors and participating cities protect FileLocal information processing operations from incidents of hardware, software or network failure resulting from carelessness, intentional abuse or accidental misuse of the system.

G. Enable management to be prepared for prudent action in the event of compromise of any security system or disaster.

2. Underlying Philosophy

This policy was written using the following rationale/philosophy:

A. FileLocal has a duty to protect its staff, information, information technology (IT) and intellectual property and an obligation to ensure vendors and participating cities provide a secure environment for employees and members of the public who have begun the process of becoming a FileLocal client.

B. Well-defined and implemented information policies and standards enable FileLocal to create secure operating environments by balancing controls and risks.

C. The level of security provided will be in line with the threat or risk and will meet the appropriate statutory and regulatory requirements.

D. Employees, and those undertaking work on behalf of FileLocal, are responsible for maintaining security over all aspects of their work and for ensuring that assets, resources and information entrusted to them are protected effectively.

E. Agency staff are expected to observe FileLocal's Code of Ethics.

F. Security is the management's accountability but the responsibility of all staff, participating cities, vendors and contractors. FileLocal understands both vendors and participating cities will have their own Information Security policies and those policies should be in alignment with the policies below and in many cases may be more than what is needed for FileLocal.

G. Information security is:

- A cornerstone of maintaining public trust
- A business concern — not a technology issue
- Risk-based and cost-effective
- Aligned with FileLocal business strategy

3. Scope

This policy applies to:

A. All FileLocal agency staff (including, but not limited to, permanent employees, contractors, temporary staff, etc.) that have access to the FileLocal service

B. Vendors and service providers (including but not limited to, permanent employees, contractors, temporary staff, etc.) responsible for the Tax Portal and Tax Payment systems which make up the FileLocal service

C. FileLocal participating cities (including but not limited to, permanent employees, contractors, temporary staff, etc.) developing and maintaining back-end data connections to the FileLocal service

D. All data and information regardless of processing mode (e.g. manual or computer) and storage mode (including but not limited to electronic or hard copy form).

E. All technologies associated with the creation, collection, processing, storage, transmission, analysis, and disposal of information

F. All data processing activities performed within or on behalf of FileLocal (including but not limited to all subsidiaries, etc.).

G. All facilities regardless of processing mode (including but not limited to batch, remote and data communication).

4. Policy Statements

A. FileLocal recognizes the immense value and importance of its staff, assets, information, and IT and is committed to ensuring their continued protection.

B. FileLocal shall seek to ensure vendors and participating cities follow IT security policies in order to protect its staff, assets, information, and information technology assets at a level appropriate to the prevailing security threat, with standards and best practice defining the minimum level of achievement.

C. Information Management shall be a consideration at the design and development stages of every business activity and not merely during implementation.

D. FileLocal shall seek to ensure vendors and participating cities make continuous improvement in methods of threat analysis and information management so that it can protect itself appropriately.

E. This policy document shall be approved by the FileLocal Executive Board, published and communicated, as appropriate, to all agency staff, vendors and participating cities.

F. This policy shall be reviewed annually, and in case of influencing changes, to ensure it remains appropriate.

G. FileLocal Information Management Policy shall comply with the FileLocal Information Management Framework and conform to ISO 17799:2005: Information Technology – Security Techniques – Code of Practice for Information Security Management. Cities can elect to use other IT Policies based on proven and adopted Federal Security standards provided those policies still meet the information management and framework adopted bythe Agency

5. Enforcement

Failure to comply with terms and conditions of the FileLocal Information Management Policy may lead to disciplinary action being taken against the individual and in some cases could result in legal proceedings. Any failure to comply with terms and conditions from a participating city could also result in a City no longer being able to use FileLocal.

6. Roles and Responsibilities

A. FileLocal

The agency is responsible for:

- Ensuring that Information Management policy is integrated into all related business operations and that information management activities are coordinated acrossthe same.
- Awareness of the company's information risk profile and ensuring that information risks are mitigated to an acceptable level in accordance with this policy.
- Ensuring that the information management strategic objectives are in alignment with the business strategy.

B. FileLocal Attorney

~~The~~ Chief Counsel is responsible for:

- Review of policies

~~.~~ FileLocal Executive with Information Security ~~responsibility:~~

C. responsibilities

The Chief Information Security Officer (CISO) or designee, or in lieu of a dedicated ~~CIS,~~ CISO, the member of FileLocal who is ultimately responsible for information security, is responsible for:

- Development and maintenance of this policy
- Development of information security principles and practices.
-

- Development and maintenance of the more detailed FileLocal IT information security policy control framework.
- Monitoring the effectiveness of information security across staff, vendors and participating cities.
- Providing the Agency with policy compliance status to statutory and regulatory requirements.

D. FileLocal Agency Staff

FileLocal is responsible for:

- Maintaining security over all aspects of their work and for ensuring that assets, resources and information entrusted to them are managed properly.
- Complying with all information management policies and procedures.
- Reporting all known or suspected security weaknesses and breaches to their line manager or the relevant security manager.

E. Vendors

Vendors are responsible for:

- Maintaining security over all aspects of their work and for ensuring that assets, resources and information entrusted to them are managed properly.
- Complying with all information management policies and procedures.
- Reporting all known or suspected security weaknesses and breaches to their line manager or the relevant security manager.
- Ensuring implementation of Information Management policies, principles and practices throughout the FileLocal service and with vendor staff

F. Participating Cities

Participating cities are responsible for:

- Maintaining security over all aspects of their work and for ensuring that assets, resources and information entrusted to them are managed properly.
- Complying with all information management policies and procedures adopted by a City's CISO, or designee,

- Reporting all known or suspected security weaknesses and breaches to FileLocal if those areas affect the connections between a city's system of record and FileLocal.
- Ensuring implementation of Information Management policies, principles and practices throughout the city staff responsible for the connections between the City system of record and FileLocal.

~~INFORMATION CLASSIFICATION POLICY (POL-010)~~

Information Classification Policy

1. Introduction

Companies process, use, and manage enormous amounts of information. Such information covers the spectrum of sensitivity, in terms of being highly valuable or less valuable, to the company and its customers. To bring a focus to protecting that which is valuable, a classification schema for information is necessary. A classification schema allows security to be directed and invested where that effort is most needed to protect the business environment. Without a classification schema, much effort would be wasted to protect information that is not cost or security justified. A classification schema should also provide both guidance to staff and the tools to apply the right level of classification to information to bring a balance of investment and attention to the overall protection responsibility.

2. Purpose

The purpose of this policy is to allow information, in its many forms, to be classified according to its degree of sensitivity and thus allow the appropriate controls to be applied to ensure its protection.

3. Scope

The Information Classification Policy applies to those who utilize the FileLocal Tax Portal owned by the Washington Multi-City Business License and Tax Portal Agency (FileLocal):

- Agency staff
- Temporary supplemental staff
- Contractors
- Vendors
- Consultants
- Participating cities
- All business partners and parties
- FileLocal system users

The Information Classification Policy also applies to all information systems, data, business applications and networks, used or administered by FileLocal and to all computational environments operated by, or operated on behalf of FileLocal.

Deviation from this policy is acceptable only if an information security threat and risk assessment has been completed with a documented business impact analysis and the Information Owner(s) have signed a risk acceptance form. The Risk Acceptance Form shall be authenticated by the Program Manager.

4. Policy ~~Statement~~Statements

A. All information shall have a designated Information Owner.

B. Information classification shall adhere to the classification scheme and guidance defined in this policy.

C. Information assets shall be classified according to:

1. Confidentiality
2. Availability
3. Integrity requirements
4. Business Impact of unauthorized disclosure

A. Information Owners shall be responsible to classify the information, whose ownership has been assigned to them.

B. Users shall be responsible to manage information relative to its classification level.

C. Information shall be labelled and safeguarded relative to its classification level

D. Information labelling shall apply to information assets in physical and electronic forms

E. Information managed within FileLocal shall be classified relative to the following hierarchy and aligns to classifications adopted at a local and State level:

1. PUBLIC
2. SENSITIVE
3. CONFIDENTIAL
4. CONFIDENTIAL, WITH SPECIAL HANDLING
5. 'CONFIDENTIAL' classification shall be the default classification.

D. Information shall be handled in accordance with the requirements set forth in the 'Information and Media Handling Standard'.

E. Information shall be retained in accordance with the requirements set forth in the 'Information Retention Standard'.

F. Information shall be destroyed once the applicable retention period has been exceeded.

G. Information shall be classified at the level of the highest component part. (For example, a document of fifty pages containing one page of 'CONFIDENTIAL' information shall be classified as 'CONFIDENTIAL').

H. The classification level of information shall be reviewed annually. Impact assessments shall be undertaken and~~/~~ / or reviewed for critical systems, or those holding 'CONFIDENTIAL' annually.

I. Information resources (i.e. systems, devices, applications) shall implement controls to be compliant with the requirements of the highest classification level of the information that it stores, processes, or transmits.

5. Roles and Responsibilities

1. PROGRAM MANAGER

The Program Manager is responsible for:

- Performing organizational self-assessment periodically to ensure compliance with this policy and related standard.
- Leading the investigation of any reported breaches in FileLocal environment in regard to inappropriate information handling.
- Ensuring that all employees are trained in regard to the applied information handling controls,

2. FILELOCAL AGENCY STAFF

FileLocal is responsible for:

- Assigning the classification category to the information, whose ownership has been assigned to the Agency.
- Maintaining an inventory of their business information for which they are responsible.
- Reviewing annually the classification level of the information for which they are responsible.
- Seeking to ensure controls are applied to their information resources, according to the resource classification category by the appropriate vendors and participating cities
- Ensuring proper management of information for which they are responsible by ensuring information retention requirements are being met by the appropriate vendors and participating cities
- Reporting information security compromises to the CISO, or designee, when inappropriate handling of information has occurred.

3. VENDORS

Vendors are responsible for:

- Assisting Information Owners to implement and manage those controls mandated by the Information Classification Policy and related artifacts.
- Assisting the Program Manager, or their designee's organizational self-assessment initiatives to confirm information classification and handling methods used, adhered to, and are implemented in accordance with this policy and related artifacts.
- Monitoring compliance to confirm currency and effectiveness of this policy and related artifacts.
- Identifying inappropriate usage of information, and the reporting thereof as incidents to the CISO, or designee.
- Assisting the Program Manager, or their designee, in investigations in regard to inappropriate handling of information.

4. PARTICIPATING CITIES

Participating Cities are responsible for:

- Assisting Information Owners to implement and manage those controls mandated by the Information Classification Policy and related artifacts as adopted by their CISO, or designee.
- Assisting the FileLocal Program Manager, or designee's, organizational self-assessment initiatives to confirm information classification and handling methods used, adhered to, and are implemented in accordance with this policy and related artifacts.
- Monitoring compliance to confirm currency and effectiveness of this policy and related artifacts.
- Identifying inappropriate usage of information, and the reporting thereof as incidents to the FileLocal Program Manager, or designee, and to a City's CISO, or designee.
- Assisting the FileLocal Program Manager, or designee, in investigations in regard to inappropriate handling of information.
- Promptly reporting violations of this policy and related standard to FileLocal Agency.
- Understanding the Information Classification Policy and related artifacts as adopted by a City CISO, or designee, and FileLocal.

6. Compliance

The Information Classification Policy uses and assimilates the following bodies of recognized knowledge: ISO 27002:2013:

- Section 8.1.1 – Inventory of Assets
- Section 8.1.2 – Ownership of Assets
- Section 8.2.1 – Classification Guidelines
- Section 8.2.2 – Labeling of information
- Section 8.2.3 – Handling of information
- Section 8.3.2 – Disposal of Media
- Section 8.3.3 – Physical Media Transfer
- Section 13.2.3 – Electronic Messaging
- Section 10 – Cryptography
- Section 18.1 – Compliance with Legal and Contractual Requirements

7. Related Documents

- Information and Media Handling Standard
- Information Retention Standard

Personnel Security Policy

1. Introduction

Secure operations of applications and systems requires the employment of trusted ~~1personnel~~personnel for administration of applications, systems, and data. Appropriate personnel must be hired, and employees must be properly educated regarding their specific information security responsibilities.

~~8.~~2. Purpose

The purpose of this policy is to outline personnel security requirements in order to ensure secure operations by FileLocal.

~~9.~~3. Scope

The Personnel Security Policy applies to all FileLocal employees, as well as any temporary contractors., and all vendors utilized by FileLocal.

Deviation from this policy is acceptable only if an information security threat and risk assessment has been completed with a documented business impact analysis and the Information Owner(s) have signed a risk acceptance form. The Risk Acceptance Form shall be authenticated by the Program Manager.

~~10.~~4. Policy Statements

A. When hiring employees for key technical positions, comprehensive pre-employment screening must take place

B. All pre-employment inquiries must be conducted in full compliance with all FileLocal and/or vendor departmental policies and in full compliance with all related state and federal laws

C. New employees must be informed about their responsibilities and the policies that apply

D. FileLocal must develop formal processes to for disciplinary actions against FileLocal employees who do not follow the requirements documented in FileLocal's information security policies and procedures

E. All employees are required to complete yearly training on the basic tenets of this information security policy

F. All physical and logical access to computing and network facilities and resources must be assigned with the principles of least privilege and separation of duties applied.

G. FileLocal must establish processes to quickly update, close, and/or remove all system and network privileges following the termination or significant change in responsibilities and privileges for any FileLocal employees.

H. Related procedures regarding employee suspension, leave of absence, long term illness or disability must also be established and maintained

~~11.~~5. Roles and Responsibilities

A. PROGRAM MANAGER

The Program Manager is responsible for:

- Performing organizational self-assessment periodically to ensure compliance with this policy and any related standards and/or procedures.
- Leading the investigation of any reported incidents in FileLocal's environment in regard to inappropriate personnel security.
- Ensuring that all employees are trained in regard to appropriate personnel security controls,

B. FILELOCAL AGENCY STAFF

FileLocal agency staff are responsible for:

- Complying with FileLocal requirements regarding personnel security
- Reporting information security compromises to the Program Manager, or their designee, when potentially inappropriate personnel security has occurred.

C. VENDORS (INCLUDING ~~E~~GOVAVENU AND KUBRA)

Vendors are responsible for:

- Implementing security controls that are mandated by this policy and related standards, for the systems of which they are in charge.
- Identifying personnel security incidents, and reporting them to FileLocal and the Program Manager, or designee.
- Assisting the Program Manager, or designee, in investigations in regard to personnel security incidents.
- Providing periodic reports to FileLocal and the Program Manager, or designee, regarding personnel security

~~12.~~6. Compliance

The Personnel Security Policy uses and assimilates the following bodies of recognized knowledge: ISO 27002:2013:

- Section 6.1.1 - Information security roles and responsibilities
- Section 7.1 – Prior to employment
- Section 7.1.1 – Screening
- Section 7.2.1 – Management Responsibilities
- Section 7.2.2 – Information security awareness, education and training
- Section 7.2.3 – Disciplinary process
- Section 7.3.1 – Termination or change of employment responsibilities

~~13.~~7. Related Documents

~~AC~~

Access Control Policy (POL 020)

1. Introduction

Users need to access data and information resources to be able to perform their daily job functions. Excessive or uncontrolled access can lead to unauthorized or unintentional disclosure and modification of business-critical information. Access to information resources should be granted to those individuals who need that particular information resource to perform their duties.

Access control must balance the restrictions to prevent unauthorized access against the need to provide unhindered access to meet business needs.

2. Purpose

The purpose of the Access Control Policy is to ensure that only authorized users access the Washington Multi-City Business License and Tax Portal Agency (FileLocal) information resources for appropriate business activities.

3. Scope

The Access Control Policy applies to those who utilize information systems, business applications, networks and information owned by FileLocal:

- Agency staff
- Temporary supplemental staff
- Contractors
- Vendors
- Consultants
- Participating cities
- All business partners and parties
- FileLocal system users

The Access Control Policy also applies to all information systems, data, business applications and networks, used or administered by FileLocal and to all computational environments operated by, or operated on behalf of FileLocal.

Deviation from this policy is acceptable only if an information security threat and risk assessment has been completed with a documented business impact analysis and FileLocal has signed a risk acceptance form. The Risk Acceptance Form shall be authenticated by the Program Manager.

4. Policy Statements

A. FileLocal shall prohibit unauthorized access, disclosure, duplication, accidental or unauthorized modification, destruction, misuse or theft of its information.

B. FileLocal shall manage access to information in its computational environment by means of an identification and authentication mechanism.

C. The data, system, application and network access assigned to each user shall be controlled on the basis of business requirements.

D. Member cities shall be authorized by FileLocal prior to being granted access to a particular resource.

E. Users shall only access resources to which they have been granted access.

F. The access control method shall be in accordance with the classification of the resource and the level of risk associated with the resource.

G. All user accounts must be based on unique identifiers that are tied to a specific person. Use of shared accounts is not allowed except when specifically authorized as a documented exception by the owner of the system in question.

H. All administrative access and access to critical/sensitive servers must be secured using multi-factor authentication.

I. User access rights shall be reviewed regularly and modified, revoked, or deactivated as appropriate.

J. User access activities shall be continuously monitored and verified regularly to detect unauthorized

K. access in a timely manner.

L. Creating and assigning access rights to users shall adhere to the following principles:

- Segregation of duties: a principle that prevents the same person from being responsible for the entire transaction end- to-end in an information system. This is done to prevent fraud and abuse of information systems.
- Least Privilege: a principle that ensures that users are granted the most restrictive set of privileges needed to perform their tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use (as opposed to granting users with widely scoped functional privileges that might grant more access than is required).
- Need to Know: a principle that ensures access to information is limited to the specific information that a user needs to know to perform authorized job duties. Similar to Least Privilege, FileLocal shall grant access to staff for only the data and information that staff legitimately need to know.

5. Roles and Responsibilities

1. PROGRAM MANAGER

The Program Manager is responsible for:

- Performing organizational self-assessment periodically to ensure compliance with this policy and related standards.

- Reviewing any technology acquisitions to determine if any clauses/statements are required in the contract with respect to compliance with this policy and related standards.
- Leading the investigation of any reported access control breaches in FileLocal computational environment.
- Ensuring that all employees are trained in regard to the applied access controls to FileLocal information resources.

2. FILELOCAL AGENCY

FileLocal is responsible for:

- Protecting information resources (i.e. data, systems, applications, network), whose ownership has been assigned to them, against unauthorized access.
- Authorizing and/or revoking privileges for access to information resources, whose ownership has been assigned to them.
- Understanding and managing access rights they have approved. As such, FileLocal shall periodically review all granted access and verify that the access continues as appropriate.
- Developing and maintaining the formal procedure for documenting, granting, changing, and terminating access to information resources, whose ownership has been assigned to them.
- Promptly reporting information security incidents to the CISO, or designee.
- Ensuring that users of their resources are complying with this policy and the associated standard and procedures. Taking the necessary corrective action where non-compliances with this policy are discovered.
- Ensuring that participating cities and vendors have undergone required security awareness training.

3. VENDORS

Vendors are responsible for:

- Implementing security controls that are mandated by this policy and related standards, for the systems of which they are in charge.
- Assisting the Program Manager, or their designee's, organizational self-assessment initiatives to confirm that FileLocal computational environment's components adhere to and are implemented in accordance with this policy and related standards.
- Identifying access control incidents, and reporting them to FileLocal and the Program Manager, or their designee.
- Assisting the Program Manager, or designee, in investigations in regard to access control breaches.
- Monitoring access control activities.
- Creating, managing, and terminating user accounts, including updating accounts when required access privileges change.

- Providing periodic reports to FileLocal and the Program Manager, or their designee.

4. PARTICIPATING CITIES

Participating Cities are responsible for:

- Accessing only the information resources to which they have been granted permission.
- Protecting FileLocal and its client's assets as an on-going responsibility of the business process and their individual task assignments.
- Identifying access control breaches and reporting them to FileLocal's Program Manager and a City's CISO, or their designee.
- Assisting the FileLocal Program Manager, or their designee, in investigations in regard to access control breaches.
- Monitoring access control activities.
- Creating, managing, and terminating user accounts.
- Providing periodic reports to FileLocal and a City's CISO, or designee.
- Promptly reporting violations of this policy and related standards (e.g. unauthorized access) to FileLocal's Program Manager and a City's CISO, or their designee.
- Understanding and following the Access Control Policy and related Standards.

6. Compliance

The Access Control Policy uses and assimilates the following bodies of recognized knowledge: ISO 27002:2013:

- Section 6.1.1 – Information Security Roles and Responsibilities
- Section 7.2.1 – Management Responsibilities
- Section 6.1.2 – Segregation of Duties
- Section 9 – Access Control

7. Related Documents

- Access Control Standard
- Identification and Authentication Standard
- Logical Access Control Standard
- Password Management Standard
- User Account Provisioning Standard

Encryption Policy (POL-030)

Introduction

Due to security exposures and risk, classified data is protected through the use of encryption technologies. Encryption technologies use complex mathematical formulae and techniques to protect the confidentiality, integrity and non-repudiation of communications and data. The Washington Multi-City Business License and Tax Portal Agency (FileLocal) uses encryption to protect classified data stored or transmitted through its information systems.

8. Purpose

The purpose of the Encryption Policy is to provide guidance on the use of encryption to ensure the confidentiality and integrity of classified information.

9. Scope

The Encryption Policy applies to those who utilize information systems, business applications, networks and information owned by FileLocal:

- Agency staff
- Temporary supplemental staff
- Contractors
- Vendors
- Consultants
- Participating cities
- All business partners and parties

The Encryption Policy also applies to all information systems, data, business applications and networks, used or administered by FileLocal and to all computational environments operated by, or operated on behalf of FileLocal.

Deviation from this policy is acceptable only if an information security threat and risk assessment has been completed with a documented business impact analysis and the Information Owner(s) have signed a risk acceptance form. The Risk Acceptance Form shall be authenticated by the Program Manager.

10. Policy Statements

A. Classified information shall always be transmitted or stored in encrypted form.

B. Cryptographic algorithms and tools shall be determined in line with policy by the Vendors in line with contractual requirements.

C. Cryptographic keys shall be protected during their entire life-cycle (generation, distribution, archiving, updating, revocation and destruction).

D. The applied cryptographic controls shall take into consideration data retention requirements.

E. Jurisdictional laws governing the use of encryption technology shall be used as legislated.

Roles and Responsibilities

1. PROGRAM MANAGER

The Program Manager is responsible for:

- Approving cryptographic algorithms, minimum key lengths, and tools for use to protect the classified FileLocal information.
- Reviewing architectural initiative(s) to determine compliance with FileLocal Encryption Policy and Standard.
- Performing organizational self-assessment annually to ensure compliance with this policy and related standard.
- Leading the investigation of any reported security breach in FileLocal computing environment.

2. FILELOCAL AGENCY

FileLocal is responsible for:

- Ensuring compliance with the encryption controls protecting the information resources.
- Ensuring that cryptographic key management is maintained according to the standard by vendors and participating cities.

3. VENDORS

Vendors are responsible for:

- Assisting Information Owners with the implementation of and the managing of encryption controls.
- Managing cryptographic keys in accordance with the requirements of this policy and related standard.
- Assisting the Executive with Information Security responsibilities' organizational self-assessment initiatives to confirm systems and infrastructure components adhere to and are implemented in accordance with this policy and related standard.
- Identifying and reporting security incidents to the Program Manager.

4. PARTICIPATING CITIES

Participating Cities are responsible for:

- Assisting Information Owners with the implementation of and the managing of encryption controls.
- Managing cryptographic keys in accordance with the requirements of this policy and related standard or managing cryptographic keys in accordance with the requirements and related standards of a City's CISO, or designee.
- Safeguarding assigned (personal) cryptographic keys.

- Immediately reporting violations of this policy (e.g. where cryptographic keys may have been compromised) to the Agency and a City's CISO, or designee.
- Understanding and following the Encryption Policy and related standard.

11. Compliance

The Encryption Policy uses and assimilates the following bodies of recognized knowledge: ISO 27002:2013:

- Section 12.3.1 – Information Back-up
- Section 13.1 – Network Security Management
- Section 13.2.1 – Information Transfer Policies and Procedures
- Section 9.4.3 – Password Management System
- Section 10 – Cryptographic Controls
- Section 18.1.5 – Regulation of Cryptographic Controls
- Section 13.1 – Network Security Management
- Section 14.1.3 – Protecting Application Services Transactions

12. Related Documents

- Encryption Standard

Infrastructure and Critical Vendor Policy (POL-040)

1. Introduction

The following policies and subsequent standards are expressly authored as foundation documents to manage Washington Multi-City Business License and Tax Portal Agency (FileLocal) infrastructure. In the marketplace reality - intrusion and unwarranted access and attacks, FileLocal must make its infrastructure safe, to protect its assets, employees, intellectual property, and taxpayer privacy. Attacks can come from external and internal sources and can cause significant loss and exposure to risks to both the business and its operations. Security controls must be in place to prevent security breaches from any source. It is unacceptable to have poorly or inadequately configured systems which can facilitate an attack and pose a high risk on critical information resources. All information systems must be deployed with secure configurations and maintained continuously to the highest standards, which are expressed in the standards documents.

2. Purpose

The purpose of the Infrastructure Policy is to articulate boundaries, scope, content, and other forms of intellectual capital that comprise FileLocal's governing principles on the security of its infrastructure, including that of critical vendors, such as ~~eGov~~Avenu and Kubra. Such expression of artifacts is intended to ensure that FileLocal's infrastructure is deployed and configured to provide the highest level of security for infrastructure components.

A second purpose is to set forth those security artifacts sufficient to ensure that security of information systems is maintained in an acceptable, useful and appropriate lifecycle.

3. Scope

The Infrastructure Policy applies to those who utilize information systems, business applications, networks and information owned by FileLocal:

- Full-time employees
- Part-time employees
- Temporary supplemental staff
- Contractors
- Consultants
- Vendors, including, but not limited to, ~~eGov~~Avenu and Kubra

The Infrastructure Policy also applies to all information systems, data, business applications and networks, used or administered by FileLocal and to all computational environments operated by, or operated on behalf of FileLocal.

Deviation from this policy is acceptable only if an information security threat and risk assessment has been completed with a documented business impact analysis and the FileLocal Agency Staff(s) have signed a risk acceptance form. The Risk Acceptance Form shall be authenticated by the Program Manager.

4. Policy Statements

A. Vendors and FileLocal shall manage their infrastructure in a manner that ensures its proper use, prevents unauthorized access or use, maintains availability and protects the security of information resources.

B. External users / systems / networks shall be allowed to connect to Vendor or FileLocal's networks only if the connection is required for a legitimate business need.

C. The security controls used by Vendors shall be commensurate with the classification level of stored, processed, or transmitted information in accordance with FileLocal's 'Information Classification Policy' and 'Information and Media Handling Standard'.

D. A formal risk assessment shall be performed on the infrastructure and critical vendors at least once a year. The risk assessment shall identify / confirm key risks imposed on the infrastructure and determine the security controls required to mitigate those risks within acceptable limits.

E. All user, system, application and network activities shall be logged to the extent that provides sufficient audit trail of those activities.

F. All documents created, stored, transmitted or received on FileLocal's computers and networks and on any attached removable devices shall be subject to monitoring by authorized personnel.

G. All security events shall be continuously monitored.

H. All monitored and logged activity on computational resources shall be reviewed by authorized personnel.

I. Equipment shall be maintained in accordance with the supplier's recommended service intervals and specifications.

5. Roles and Responsibilities

A. PROGRAM MANAGER

The Program Manager is responsible for:

- Developing and implementing strategies to ensure users are aware of using security policies, procedures, and benefits.
- Performing organizational self-assessment periodically to ensure compliance with this policy and related artifacts.
- Periodically evaluating effectiveness of security policies and procedures.
- Reviewing any planned technology acquisition(s) to determine if any clauses / statements are required in the contract with respect to compliance with FileLocal's security policies and standards.
- Reviewing any architectural initiative(s), including selecting vendors, to determine compliance with FileLocal's security policies and standards.
- Leading any investigation of any reported security breaches in FileLocal's or Critical Vendors' systems business applications or networks.
- Authorizing inbound and outbound traffic through the firewall - as needed by the business.

B. FILELOCAL AGENCY STAFF

FileLocal Agency Staffs are responsible for:

- Ensuring FileLocal's computational resources are configured to adhere to the controls mandated by this policy and related standards, where ownership has been assigned to them.
- Establishing and maintaining an inventory of computational resources (e.g. servers, desktops, laptops, network devices).
- Authorizing access privileges to the computational resources, where such ownership has been assigned to them.
- Promptly reporting security incidents to the FileLocal Executive with Information Security Responsibilities.
- Monitoring the quality of any IT service provided by Third Parties to ensure compliance with the SLA.
- Ensuring compliant security logging is implemented on the computational resources.
- Ensuring team members are compliant with this policy and related artifacts.
- Proceeding with necessary corrective actions where policy non-compliance has occurred with team members.
- Ensuring changes to those owned computational resources are documented and implemented.

C. CRITICAL VENDORS (INCLUDING ~~ECOV~~ AVENU AND KUBRA)

Critical Vendors are responsible for:

- Assisting FileLocal Agency Staff to implement and maintain security controls mandated by this policy and related artifacts.
- Providing assistance to the FileLocal Executive with Information Security Responsibilities' organizational assessment initiatives to confirm systems and infrastructure components adhere to and are implemented in accordance with this policy and related standards and procedures.
- Assisting Information Users on the use of infrastructure resources and solving technical problems in accordance with FileLocal Infrastructure Policy and Standards.
- Keeping up-to-date documentation pertaining to the infrastructure architecture and infrastructure components.
- Monitoring user, network and system activities; maintain the audit logs and ensure its continuous integrity.
- Performing security scans of perimeter devices bi-annually, to detect – non-compliance (e.g. unauthorized modems).
- Reviewing the configuration of infrastructure components on a regular basis.
- Identifying any non-compliant computational activities, and report such to FileLocal Agency Staff and the FileLocal Executive with Information Security Responsibilities.

- Recording security incidents relating to the infrastructure, report them to the FileLocal Executive with Information Security Responsibilities.
- Providing assistance to the FileLocal Executive with Information Security Responsibilities for investigations of security breaches in regard to the infrastructure.
- Providing periodic reports to FileLocal Agency Staffs and the FileLocal Executive with Information Security Responsibilities.

D. INFORMATION USERS

Information Users are responsible for:

- Accessing only those information resources to which they have been granted permission.
- Accessing FileLocal's information resources and Internet only via approved access points.
- Protecting access credentials and safeguarding portable computers from loss / theft.
- Protecting sensitive / confidential information on devices assigned to them.
- Ensuring that the use of computational resources (e.g. their devices, network devices, servers, etc) is in compliance with the requirements mandated by this policy and related standards.
- Immediately reporting violations of this policy and related standards to Help Desk.
- Working within and respecting the intention / purpose /objectives of this Policy and related artifacts.
- Not changing or altering system and application security configuration of their computers/devices.
- Protecting FileLocal's and FileLocal's client information as a regular part of the business process and their individual work assignments.

6. Compliance

The Infrastructure Policy uses and assimilates the following bodies of recognized knowledge: ISO 27002:2013:

- Section 8.1 - Responsibility for assets
- Section 11.1 - Secure areas
- Section 11.2 - Equipment
- Section 12.1 - Operational procedures and responsibilities
- Section 12.1.3 Capacity Management
- Section 12.3 – Backup
- Section 12.4 – Logging and Monitoring
- Section 13 – Communications Security
- Section 13.1 - Network security management

- Section 14.2.9 System Acceptance Testing
- Section 15.2 - Supplier Service Delivery Management

7. Related Documents

- Remote Access Standard
- Perimeter Security Standard
- Wireless Standard
- Security Event Monitoring Standard
- Audit Trail Standard
- Laptop, PDA and Mobile Devices Standard
- Network and Network Devices Standard
- Server, Desktop and Mainframe Standard
- Vulnerability Management Standard
- System Hardening Standards

Physical and Environmental Security Policy (POL-050)

1. Introduction

Information resources require not only logical but also physical security controls to protect the confidentiality, integrity and availability of information and ensure proper and timely operation. Computer systems and facilities shall be protected from theft, unauthorized disruption of operation and damage caused by environmental hazards such as fire, dust, water, and other contaminants or the unplanned loss of power.

2. Purpose

The purpose of the Physical and Environmental Policy is to outline the principles that govern the implementation of physical security controls that protects the Washington Multi-City Business License and Tax Portal Agency (FileLocal) information resources. As the FileLocal staff utilize the City of Seattle's infrastructure for day-to-day work, the FileLocal staff are under the City of Seattle's CISO, or designee, policies around Physical and Environment as well. This policy is to further refine the specifics for the agency as a separate Municipal Non-Profit Corporation.

3. Scope

The Physical and Environmental Policy applies to those who utilize information systems, business applications, networks and information owned by FileLocal:

- Agency staff
- Temporary supplemental staff
- Contractors
- Vendors
- Consultants
- Participating cities
- All business partners and parties

The Physical and Environmental Policy also applies to all information systems, data, business applications and networks, used or administered by FileLocal and to all computational environments operated by, or operated on behalf of FileLocal.

The policy also applies to all facilities and physical areas that host any kind of information resources.

Deviation from this policy is acceptable only if an information security threat and risk assessment has been completed with a documented business impact analysis and FileLocal has signed a risk acceptance form. The Risk Acceptance Form shall be authenticated by the Program Manager.

4. Policy Statements

A. The applied physical access controls shall be commensurate with the identified risk and its impact on business processes.

B. Access to business facilities and restricted areas shall be restricted to authorized personnel only.

C. FileLocal shall ensure strong physical controls around handling visitors that access FileLocal colocation facilities.

D. FileLocal shall adopt clear desk practices according to the “Physical and Environmental Policy”.

E. FileLocal shall ensure physical intrusion detection system and surveillance systems (for example, CCTV), as appropriate to safeguard restricted colocation areas.

F. FileLocal shall apply appropriate safeguards against disruptive events such as fire, flood, and other environmental hazards.

G. FileLocal shall apply automatic alarm systems as necessary to notify Facility Security about environmental hazards.

H. FileLocal shall protect computer media and other information processing systems against theft.

I. Temperature and humidity shall be controlled in data processing facilities.

J. Equipment, information, and software shall not be taken off-site without appropriate authorization under the “IT Asset Management Policy”.

5. Roles and Responsibilities

A. Program Manager

The Program Manager is responsible for:

- Performing organizational self-assessment periodically to ensure compliance with this policy and related standard.
- Ensuring that all employees are trained in regard to the applied physical controls to FileLocal information resources.

B. FileLocal

FileLocal is responsible for:

- Protecting information resources (i.e. data, systems, applications, network), whose ownership has been assigned to them, against physical and environmental threats as well as unauthorized physical access
- Authorizing access to security areas that host information resources whose ownership has been assigned to them.

C. Vendors

Vendors are responsible for:

- Implementing security controls that are mandated by this policy and related standards, for the systems of which they are in charge.

Assisting Executive with Information Security responsibilities organizational self-assessment initiatives to confirm that FileLocal computational environment's components adhere to and are implemented in accordance with this policy and related standard.

D. PARTICIPATING CITIES

Participating Cities are responsible for:

- Following the security protocols established by a City's CISO, or designee, and ensuring the overlying policy is met.

6. Compliance

The Physical and Environmental Security Policy uses and assimilates the following bodies of recognized knowledge: ISO 27002:2013:

- Section 11.1.1 – Physical security perimeter
- Section 11.1.2 – Physical entry controls
- Section 11.1.3 – Securing offices, rooms, and facilities
- Section 11.1.4 – Protecting against external and environmental threats
- Section 11.1.5 – Working in secure areas
- Section 11.2.1 – Equipment siting and protection
- Section 11.2.3 – Cabling security
- Section 11.2.5 – Removal of property
- Section 11.2.9 – Clear Desk and Clear Screen Policy

7. Related Documents

- N/A

Third Party Management and Outsourced Services Policy (POL-060)

1. Introduction

In many situations, outsourcing offers a company a cost-effective alternative to in-house capabilities. Outsourcing, however, does not reduce the fundamental risks associated with information technology or the business lines that use it. On the contrary, engaging external parties introduces new risk factors as the company's mandate to protect its business-critical information partly relies on the security controls applied by the service provider.

Similarly, Third Party access to a company's information resources imposes risk on the integrity, confidentiality and availability of information and the continuity of business operation.

2. Purpose

The purpose of the Third-Party Management and Outsourced Services Policy is to ensure contiguous security of Washington Multi-City Business License and Tax Portal Agency's (FileLocal's) information resources with respect to its computational environment when dealing with third parties and contracted entities.

~~2.~~3. Scope

The Third-Party Management and Outsourced Services Policy applies to those who utilize information systems, business applications, networks and information owned by FileLocal:

- Agency Staff,
- Temporary supplemental staff,
- Contractors,
- Consultants,
- All business partners and third parties, including Critical Vendors, such as e-Gov and Kubra.

The Third-Party Management and Outsourced Services Policy also applies to all information systems, data, business applications and networks, used or administered by FileLocal and to all computational environments operated by, or operated on behalf of FileLocal.

The document will use "Third Parties" as a collective term to denote:

- Third parties not under contractual terms to FileLocal but providing a service to FileLocal as mutually agreed.
- Approved Third Parties that are to provide FileLocal with a commercial service under a yet to be executed agreement.
- Subcontractors providing services to FileLocal as employee equivalents or staff augmentation, who are obligated under master agreements, individual agreements and/or other such contracts.
- Trading Partners, (may or may not be within a mutually executed contract).
- Suppliers of products, services (including network services) and information.

- Suppliers of remote systems support and maintenance.
- Customers, as they may wish to conduct a commercial transaction in advance of or not requiring a form of contract,
- Any other entity needing to connect with FileLocal computational environment to provide a service as mutually agreed.

Deviation from this policy is acceptable only if an information security threat and risk assessment has been completed with a documented business impact analysis and the Information Owner(s) have signed a risk acceptance form. The Risk Acceptance Form shall be authenticated by the Program Manager.

~~3.~~4. Policy Statements

1. IT services shall be obtained from service providers that are capable of providing effective security controls.
2. Third party access and outsourced services shall be supported by documented contracts and/or service level agreements. These agreements shall:
   - Define the security service level commitments by the IT service provider and each Third Party.
   - Identify responsibilities for all parties involved, including responsibilities with respect to legal matters.
   - Mandate each Third Party's compliance with FileLocal's Information Management Policies and Standards.
   - Promote compliance with corporate governance, legal and regulatory requirements.
   - Govern the cooperation on investigation efforts of security incidents.
3. FileLocal shall require approval to the use of a third party's computational resources in advance of remote or internal access to FileLocal's computational resources.
4. The Confidentiality, Integrity and Availability of data shall be protected over connections with Third Parties and on computational resources owned by Third Parties. The level of protection required shall be determined by assessing the risk to business requirements.
5. No Third -Party connection shall be authorized without evidence that relevant Information Owner(s) have completed a formal assessment and acceptance of the risk to the shared infrastructure.
6. Third Parties shall access FileLocal's computational resources using hardware, software and network components as per agreement.
7. Third Party's artifacts including, but not limited to, risk assessment document, configuration details, etc. shall be maintained and access provided to authorized staff only.
8. Information Owners shall monitor the security of service provided by each Third Party and ensure compliance with the contracted SLA.
9. Any change in a Third Party's access shall follow FileLocal's Change Management Process. Security and privacy concerns of FileLocal shall be addressed in the change management process performed by the vendor.

10. FileLocal shall have the right to audit the security measures at each Third Party and third party devices accessing FileLocal's computational resources, or be provided with the most recent external audit of Third Party's information system SSAE 18, SOC 2 related to the service being provided to ensure compliance with the agreement.
11. Each Third -Party connection shall be reviewed regularly to confirm a continuing business need.
12. Each Third -Party access shall be removed immediately, when the business relationship with that Third Party terminates / ceases or Third Party's access is no longer required.
13. Third Parties shall receive appropriate training and regular updates in FileLocal's information security policies and standards. This includes security requirements, legal responsibilities, and business controls, as well as training in the correct use of information processing facilities, before access to information or services is granted.
14. Third Party agents working in secure areas shall be supervised at all times to prevent opportunities for malicious activities.
15. Non-disclosure agreements should be signed where appropriate.

4.5. Roles and Responsibilities

5.1 Program Manager

The Program Manager is responsible for:

- Performing organizational self-assessment periodically to ensure compliance with this policy and related standards.
- Periodically evaluating the effectiveness of security policies and procedures.
- Reviewing any third -party agreement(s) to determine compliance with FileLocal information security policies and standards.
- Leading the audit exercise against Third Party information resources.
- Leading the investigations in regard to Third Party access control breaches.

5.2 FileLocal

FileLocal is responsible for:

- Assessing risk arising from Third Party access.
- Authorizing Third Party access to information resources, whose ownership has been assigned them.
- Revoking authorization for Third Party access when the business/contractual relationship ends.
- Promptly reporting information security incidents to the Executive with Information Security responsibilities.
- Monitoring the security of service provided by each Third Party to ensure compliance with the SLA.

- Ensuring that Third Party users of their resources are complying with this policy and taking the necessary corrective action where deviation from this policy is discovered.
- Ensuring that security and privacy concerns are addressed at all parts of the project management process.

5.3 Critical Vendors (Including, but not limited to, e-Gov and Kubra)

Critical Vendors are responsible for:

- Ensuring that Third Parties working with FileLocal information resources follow this policy.
- Assisting the Executive with Information Security Responsibilities' organizational self-assessment initiatives to confirm that FileLocal computational environment's components adhere to and are implemented in accordance with this policy.
- Identifying access control breaches, and reporting them to Information Owners and the Executive with Information Security responsibilities.
- Assisting the Executive with Information Security responsibilities in investigations in regard to Third Party access control breaches.
- Monitoring access control activities.
- Creating, managing and terminating Third Party user accounts.
- Providing periodic reports to FileLocal and the Executive with Information Security responsibilities.
- Ensuring that security and privacy concerns are addressed at all parts of the project management process

~~5.~~6. Compliance

The Third-Party Management and Outsourced Services Policy uses and assimilates the following bodies of recognized knowledge: ISO 27002:2013:

- **Section** 6 – Organization of Information Security
- Section 7.2.2 - Information security awareness, education, and training
- Section 9.1 - Business Requirement for Access Control
- Section 9.2 - User Access Management
- Section 9.4 – System and application access control
- Section 11.1.2 - Physical entry controls
- Section 12.4.1 - Event logging
- Section 13.1.1 – Network Controls
- Section 13.2.4 - Confidentiality or non-disclosure agreements
- Section 15.1.2 - Addressing security within supplier agreements

~~6.~~7. Related Documents

- N/A

Data Backup (POL-070)

1. Introduction

Each company faces multiple intentional and unintentional threats that could cause the loss, corruption, or temporary unavailability of data such as hardware failures, accidental deletion, incorrect modification, software corruption, and malicious activities. As these threats occur quite frequently, it is essential that backup copies of business -critical information are maintained diligently. Backup copies ensure the continued availability and viability of the information when these threats occur.

2. Purpose

The purpose of the Data Backup Policy is to outline the principles that govern the implementation of backup and recovery controls, which ensure the availability of the Washington Multi-City Business License and Tax Portal Agency (FileLocal) information resources.

3. Scope

The Data Backup Policy applies to those who utilize information systems, business applications, networks and information owned by FileLocal:

- Agency staff
- Temporary supplemental staff
- Contractors
- Vendors
- Consultants
- Participating cities
- All business partners and parties

The Data Backup Policy also applies to all information systems, data, business applications and networks, used or administered by FileLocal and to all computational environments operated by, or operated on behalf of FileLocal.

Deviation from this policy is acceptable only if an information security threat and risk assessment has been completed with a documented business impact analysis and the FileLocal have signed a risk acceptance form. The Risk Acceptance Form shall be authenticated by the Executive with Information Security responsibilities.

4. Policy Statements

A. FileLocal business critical information shall be backed up so that it can be restored when required.

B. Data backup periods shall be defined based on business requirements. These requirements shall be determined based on the acceptable data loss in case of a disruption.

C. When the acceptable data loss is less than the period between the backup jobs, backups shall be coupled with other information retention methods (e.g. transaction logs, mirroring, clustering, and fail-over capabilities).

D. Backup retention shall be implemented in accordance with the "Information Retention Standard".

E. Backups have the same sensitivity level as the data stored on them, according to the Information Classification Policy.

F. FileLocal shall regularly test the backup and restore procedures and equipment.

G. Backup media shall be handled in accordance with the Data Storage Media Library Management Policy and all current vendor contracts

H. Off-site backup shall be maintained in a secure location, separate from FileLocal data center.

I. Security controls for media held at remote locations shall be the same as at the main sites.

J. FileLocal shall develop and implement detailed procedures for performing backups, restoring data, performing testing of backups, transferring tapes to/from the storage facility, and recycling or disposing of backups upon expiration of their retention period.

5. Roles and Responsibilities

A. FileLocal Executive with Information Security responsibilities Executive with Information Security responsibilities is responsible for:

- Performing organizational self-assessment periodically to ensure compliance with this policy and related artifacts.
- Leading investigations of any reported control breaches with regards to data backup and restoration.
- Ensuring that all FileLocal staff are trained with regards to the applied data backup controls.

B. FileLocal

FileLocal is responsible for:

- Ensuring that data, whose ownership has assigned to them, are backed up in accordance to this policy and related artifacts.
- Ensuring that formal procedures for data backup and restoration are developed.
- Promptly reporting information security incidents to the Executive with Information Security responsibilities.

C. Vendors

Vendors are responsible for:

- Implementing security controls that are mandated by this policy and related artifacts, for the systems of which they are in charge.
- Backing up and restoring any FileLocal information stored on their systems.

- Assisting Executive with Information Security responsibilities organizational self- assessment initiatives to confirm that FileLocal computational environment's components adhere to and are implemented in accordance with this policy and related artifacts.
- Responding to access control breaches and reporting them to FileLocal and the Executive with Information Security responsibilities.
- Assisting the Executive with Information Security responsibilities in investigations of breaches with regards to data backup and restoration.
- Developing and maintaining data backup procedures.

D. Participating Cities

Participating Cities are responsible for:

- Ensure that systems of record have appropriate storage and backup facilities. An annual attestation to this will be sent FileLocal annually.
- Understanding and following the Data Backup Policy and related artifacts and following a City's CISO, or designee, Information Security polices related to data backup.

6. Compliance

The Data Backup Policy uses and assimilates the following bodies of recognized knowledge: ISO 27002:~~2005~~2013:

- Section 7.1.2 – Ownership of assets
- Section 7.2.2 – Information labeling and handling
- Section 9.1.2 – Physical entry controls
- Section 10.5.1 – Information back-up
- Section 10.7 – Media Handling

7. Related Documents

- Information Retention Standard

Storage Media Library Management Policy (POL-070)

1. Introduction

Critical information is stored on backup tapes and other media as part of the Washington Multi-City Business License and Tax Portal Agency (FileLocal) operational procedures. The media must be protected from unauthorized disclosure, abuse and physical damage as information stored on these media is subjected to a variety of human and environmental threats.

2. Purpose

The purpose of the Data Storage Media Library Management Policy is to outline the principles that govern the implementation of media library management controls to protect the content of the storage media.

3. Scope

The Data Storage Media Library Management Policy applies to those who utilize information systems, business applications, networks and information owned by FileLocal:

- Agency staff
- Temporary supplemental staff
- Contractors
- Vendors
- Consultants
- Participating cities
- All business partners and parties, including critical vendors, such as e-Gov and Kubra.

The Policy also applies to all information systems, data, business applications and networks, used or administered by FileLocal and to all computational environments operated by, or operated on behalf of FileLocal.

The Data Storage Media Library Management Policy applies to all data storage media such as magnetic tapes, magnetic or optical cartridges, disks and diskettes, or solid -state storage technologies.

Deviation from this policy is acceptable only if an information security threat and risk assessment has been completed with a documented business impact analysis and the FileLocal have signed a risk acceptance form. The Risk Acceptance Form shall be authenticated by the Program Manager.

~~4.~~

~~5.~~4. Policy Statements

A. FileLocal shall be able to track the content, location, security classification (for example, copying restrictions) and identification of FileLocal data for all media.

B. All media shall be labelled with a unique identifier, ownership information, security classification, and any necessary handling requirements.

C. If no longer required, the previous contents of any reusable media to be removed from FileLocal shall be sanitized.

D. Authorization shall be required for any media to be removed from FileLocal premises. A record of all such removals shall be kept to ensure accountability.

E. All media shall be stored in a safe, secure environment, in accordance with manufacturers' specifications and regulatory requirements.

F. All information stored on media shall be protected according to the Information Classification Policy and related standard.

~~6.~~5. Roles and Responsibilities

A. PROGRAM MANAGER

The Program Manager is responsible for:

- Performing organizational self-assessment periodically to ensure compliance with this policy and related standards.
- Leading the investigation of any reported breaches in FileLocal computational environment in regard to media library management.
- Ensuring that appropriate personnel are trained in regard to the applied media library management controls.

B. FILELOCAL

FileLocal is responsible for:

- Performing organizational self-assessment periodically to ensure compliance with this policy and related standards.
- Leading the investigation of any reported breaches in FileLocal computational environment in regard to media library management.
- Ensuring that appropriate personnel are trained in regard to the applied media library management controls.

C. VENDORS

Vendors are responsible for:

- Implementing security controls that are mandated by this policy and related artefacts, for the systems of which they are in charge.
- Assisting Executive with Information Security responsibilities organizational self-assessment initiatives to confirm that FileLocal computational environment's components adhere to and are implemented in accordance with this policy and related standards.
- Identifying control breaches in regard to media library management (e.g. missing media or any deviation to this policy~~))~~, and reporting them to FileLocal and the Executive with Information Security responsibilities.
- Assisting the Executive with Information Security responsibilities in investigations in regard to media library management breaches.
- Understanding and following the requirements mandated by this policy and related artifacts.

D. PARTICIPATING CITIES

Participating Cities are responsible for:

- Assisting the Executive with Information Security responsibilities in investigations in regard to media library management breaches.
- Understanding and following the requirements mandated by this policy and related artifacts and following a City's CISO, or designee, information security policies related to this policy.

~~7.~~6. Compliance

The Data Storage Media Library Management Policy uses and assimilates the following bodies of recognized knowledge: ISO 27002:2013:

- Section 8.1.1 – Inventory of assets
- Section 8.1.2 – Ownership of assets
- Section 8.2.2 – Labeling of information
- Section 8.2.3 – Handling of assets
- Section 11.2.5 – Removal of assets
- Section 8.3.1 – Management of removable media
- Section 8.3.2 – Disposal of media
- Section 8.3.3 – Physical media transfer
- Section 12.4.1 – Audit logging
- Section 9.2 – User Access Management

~~8.~~7. Related Documents

- N/A

Compliance (POL-090)

1. Introduction

The management of information and the design, operation, use of and management of information systems are subject to statutory, regulatory and contractual security requirements. The Washington Multi-City Business License and Tax Portal Agency (FileLocal) is legally obligated to comply with such regulations and to ensure to its stakeholders that criteria are met or surpassed.

2. Purpose

The purpose of this policy is to ensure compliance with statutory and regulatory requirements and alignment with ISO Standard Information technology — Security techniques — Code of practice for information security management (ISO 27002:~~2005~~2013) and industry best practices such as Control Objectives for Information and related Technology (COBIT) version 4.

3. Scope

The Compliance Policy applies to those who utilize information systems, business applications, networks and information owned by FileLocal:

- Agency staff
- Temporary supplemental staff
- Contractors
- Vendors
- Consultants
- Participating cities
- All business partners and parties

The Compliance Policy also applies to all information systems, data, business applications and networks, used or administered by FileLocal and to all computational environments operated by, or operated on behalf of FileLocal.

Deviation from this policy is acceptable only if an information security threat and risk assessment has been completed with a documented business impact analysis and the FileLocal have signed a risk acceptance form. The Risk Acceptance Form shall be authenticated by the Executive with Information Security responsibilities.

4. Policy Statements

A. Statutory, regulatory and contractual requirements shall be defined and documented for use by information, computational resources and processes. Note that legislative requirements vary from country to country and may vary when information is intended for trans-border data flow, e.g. created in one country then transmitted to another country.

B. Changes in all relevant statutory, regulatory and contractual requirements shall be reviewed on a regular basis.

C. Changes in the information management policies shall be in accordance with FileLocal operating procedures.

D. Legal restrictions shall apply to the usage of material with any associated intellectual property rights, such as copyright, trademarks, patents.

E. FileLocal records shall be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

F. Data protection and privacy shall adhere to relevant legislation, regulations.

G. Cryptographic controls shall be applied to comply with relevant agreements, laws, and regulations.

H. Software license conditions shall be validated annually.

I. FileLocal staff, contractors, and service providers shall comply with FileLocal information security policies, standards, procedures and guidelines.

J. Users shall be educated on, monitored for, and reported on unauthorized use of FileLocal computational resources.

K. Agency staff awareness shall be reinforced annually on information security policies and standards and disciplinary actions for non-compliance.

L. External Third-Party expert resources shall perform annual reviews to ensure compliance to FileLocal information security policies and standards.

M. Information management policies and standards shall be reviewed annually and updated~~,~~ as necessary.

N. Information security procedures and guidelines shall be reviewed semi-annually and updated~~,~~ as necessary.

O. Compliance assessments shall be planned to minimize risk and disruptions to business processes.

5. Roles and Responsibilities

A. Chief Information Officer

Chief Information Officer (CIO) is responsible for:

- Ensuring compliance with software licensing.

B. Executive with Information Security responsibilities

Executive with Information Security responsibilities is responsible for:

- Performing organizational self-assessment periodically to ensure compliance with this policy and related standards.
- Leading the investigation of any reported non-compliance issues.
- Ensuring that all employees are trained in regard to the applied controls and disciplinary actions for non-compliance~~,~~.

- Defining relevant statutory, regulatory and contractual obligations into compliance requirements.
- Identifying relevant changes from authorized sources that affect FileLocal information security policies, and standards.
- Reviewing policies, standards annually.

C. FileLocal

FileLocal is responsible for:

- Ensuring information and computational resources within their areas of responsibility are handled and managed to achieve compliance with FileLocal information security policies and standards.
- Reporting suspected security compromises for non-compliance to the Executive with Information Security responsibilities.

D. Vendors

Vendors are responsible for:

- Implementing security controls that are mandated by this policy and related standards, for the systems of which they are in charge.
- Assisting Executive with Information Security responsibilities organizational self- assessment initiatives to confirm that FileLocal computational environment's components adhere to and are implemented in accordance with this policy and related standards.
- Immediately reporting security compromises / non-compliance to the Executive with Information Security responsibilities.
- Assisting the Executive with Information Security responsibilities in investigations in regard to access control breaches.

E. Participating Cities

Participating Cities are responsible for:

- Respecting intellectual capital / property rights.
- Using software legally.
- Promptly reporting violations of FileLocal information security policies and standards to Help Desk.
- Adhering to FileLocal information security policies and standards.

F. Internal Audit

Internal Audit is responsible for:

- Ensuring adherence to information security policies and standards through periodic compliance assessments.

6. Compliance

The Compliance Policy uses and assimilates the following bodies of recognized knowledge: ISO 27002:~~2005~~2013:

- Section 6.1.8 – Independent Review of Information Security
- Section 7.1.3 – Acceptable use of Assets
- Section 10.1.2 – Change Management
- Section 15.1 – Compliance with Legal Requirements
- Section 15.1.2 – Intellectual Property Rights
- Section 15.1.3 – Protection of organizational records
- Section 15.1.4 – Data Protection and Privacy of Personal Information
- Section 15.1.5 – Prevention of Misuse of Information Processing Facilities
- Section 15.1.6 – Regulation of Cryptographic Controls
- Section 15.2.1 – Compliance with Security Policies and Standards
- Section 15.2.2 – Technical Compliance Checking
- Section 15.3.1 – Information Systems Audit Controls

7. Related Documents

- Acceptable Use Standard
- Security Assessment and Audit Standard

Incident Response Policy (POL-100)

1. Introduction

Businesses are subject to intrusions by unauthorized parties more than ever for a variety of reasons. Responding to security incidents and security events is an important component of the Washington Multi-City Business License and Tax Portal Agency (FileLocal) information security operations.

A strategy for managing security incidents requires the use of technologies and business practices aimed at prevention and mitigation. Preventive activities are based on measuring risk and applying various means to lower the number of security incidents and minimize anticipated resultant damage. Regrettably, not all security incidents can be prevented. To mitigate and manage a security incident requires a security incident response and reaction capability that is necessary to rapidly detect incidents, minimize loss and destruction, restore the assets as soon as possible, and improve practices based on the weaknesses exploited.

2. Purpose

The purpose of the security Incident Response Policy is to provide direction as to FileLocal preferred approaches to managing security incidents to protect assets and resources. FileLocal security Incident Response Policy is intended to frame processes and resources (trained staff) to manage security related problems and incidents to minimize business impacts professionally, including:

- Responding to incidents systematically.
- Helping personnel to recover quickly and efficiently from security incidents.
- Using information and knowledge gained during security incident to better manage and prepare for potential future security incidents.

3. Scope

The Incident Response Policy applies to those who utilize information systems, business applications, networks and information owned by FileLocal:

- Agency staff
- Temporary supplemental staff
- Contractors
- Vendors
- Consultants
- Participating cities
- All business partners and parties

The Incident Response Policy also applies to all information systems, data, business applications and networks, used or administered by FileLocal and to all computational environments operated by, or operated on behalf of FileLocal.

A 'Security Incident' is an adverse event that compromises the security of a system, a network, information, physical assets, and/or the safety of employees. A 'Security Incident' includes malicious activities such as viruses, hacker attacks, stealing hardware or software or other assets, and unauthorized access to classified information. Security Incidents are categorized as follows:

- Physical (Threat or intrusion)
- Logical (attempts or actual unauthorized intrusions)
- Compliance based
- Awareness based

Deviation from this policy is acceptable only if an information security threat and risk assessment has been completed with a documented business impact analysis and the FileLocal have signed a risk acceptance form. The Risk Acceptance Form shall be authenticated by the Program Manager.

4. Policy Statements

A. All Security Incidents shall be responded to as they occur or become known to FileLocal.

B. Incidents shall be categorized and prioritized based on the impact of the problem on the business.

C. Security Incidents shall be reported immediately in the following manner:

   I Users and Contracted Service Providers shall report a security incident to the Help Desk. II FileLocal and Custodians shall report security incidents to the Program Manager.

D. FileLocal supports a 'Whistle Blower' arrangement where the Program Manager shall receive a suspected security incident notification in secret.

E. FileLocal staff shall receive regular training relating to the action steps to be performed in the event of a security incident.

F. Incident response activities shall be escalated if necessary so that further damage can be avoided.

G. FileLocal staff, participating cities and suppliers shall have a plan for escalation and notification, based on the impact of the problem on the business.

H. Contact information and points of contact with law enforcement authorities, regulatory bodies, information service providers and media shall be maintained.

I. Vendors shall investigate and identify the causes of incidents, based on the impact and risk for the business.

J. Chain of custody shall be followed to be able to present the evidence in court.

K. Vendors shall form a Computer Security Incident Response Team.

L. Vendors shall apply appropriate diagnostic tools for effectively diagnosing the causes of an incident.

M. Third party contracts shall support cooperation on investigation efforts on security incidents.

N. Security incident response process shall be monitored to ensure compliance.

O. Roles and Responsibilities

A. PROGRAM MANAGER

The Program Manager is responsible for:

- Working with law enforcement authorities.
- Engaging Corporate Communications to ensure only appropriate information is released.
- Maintaining contacts with law enforcement authorities, regulatory bodies, information service providers and media.

B. FILELOCAL

FileLocal is responsible for:

- Promptly reporting information security incidents to the Executive with Information Security responsibilities.
- Ensuring security incident response procedures are in place and useful for their resources.
- Providing ongoing support and resources to Computer Security Incident Response Team (CSIRT).

C. VENDORS

Vendors are responsible for:

- Implementing security controls that are mandated by this policy and related standard, for the systems of which they are in charge.
- Assisting Executive with Information Security responsibilities organizational self- assessment initiatives to confirm that FileLocal computational environment's components adhere to, and are implemented in accordance with this policy and related standard.
- Contributing constructively to security incident response procedures to make them efficient and useful.
- Documenting activities and observations used in the security incident response process, to contribute to incident response best practice improvements.
- Determining incidents that meet 'false positive' criteria.
- Communicating security incident alerts to the Executive with Information Security responsibilities.
- Providing technical expertise, as a resource, to CSIRT.
- Performing organizational self-assessment periodically to ensure compliance with this policy and related standard.
- Assessing, categorizing and analyzing security incidents.
- Leading security investigations.
- Directing the Computer Security Incident Response Team.
- Escalating security incidents~~,~~ as necessary.
- Providing recommendations to resolve security incidents.

- Ensuring the cause of security incidents has been identified and addressed.
- Ensuring security incidents are resolved.
- Communicating / disseminating security incident information / reports to Executive Management, affected users and clients as required.
- Ensuring security incident response activities are documented.
- Ensuring staff receive training to ensure incident response procedures are understood.
- Ensuring that related processes (e.g. Incident Response, Escalation and Notification processes) are in place and useful and can be invoked as an intermittent unscheduled business process.
- Ensuring a repository of occurred security incidents is maintained.
- Ensuring the chain of custody is followed.

5. Participating Cities

Participating Cities are responsible for:

- Promptly reporting security incidents to Help Desk and to a City's CISO, or designee, in accordance to the Information Security Policies adopted.
- Co-operating with and contributing to the security incident response activities as required.

6. Compliance

The Incident Response Policy uses and assimilates the following bodies of recognized knowledge: ISO 27002:2013:

- Section 6.1.3 – Contact with Authorities
- Section 15.1.2 – Addressing security within supplier agreements
- Section 8.2.1 – Classification of information
- Section 16.1.1 – Responsibilities and procedures
- Section 16.1.2 – Reporting information security events
- Section 16.1.6 – Learning from information security incidents
- Section 16.1.7 – Collection of evidence

7. Related Documents

- Incident Response Procedure

Security Risk Assessment (POL-110)

1. Introduction

Information Security Risk Assessments (RA) are a necessary component to understanding the overall susceptibility of the organization to negative outcomes during normal operations. Assessment of risk utilizing a well understood methodology will produce results which can be compared on a timeline basis.

2. Purpose

To require the Washington Multi-City Business License and Tax Portal Agency (FileLocal) to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

3. Scope

The Security Risk Assessment Policy applies to those who utilize information systems, business applications, networks and information owned by FileLocal:

- Agency staff
- Temporary supplemental staff
- Contractors
- Vendors
- Consultants
- Participating cities
- All business partners and parties

The Security Risk Assessment Policy also applies to all information systems, data, business applications and networks, used or administered by FileLocal and to all computational environments operated by, or operated on behalf of FileLocal.

Deviation from this policy is acceptable only if an information security threat and risk assessment has been completed with a documented business impact analysis and the FileLocal have signed a risk acceptance form. The Risk Acceptance Form shall be authenticated by the Chief Information Security Officer (CISO), or designee.

4. Policy Statements

A. All RA activities shall be conducted under a single planning authority to ensure that full coverage of the environment is maintained.

B. RAs shall be conducted on any information system, including applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained

C. RAs shall be conducted not more than annually.

D. RAs shall be conducted on any entity which has signed a third -party agreement with FileLocal.

E. The execution, development and implementation of remediation programs is the joint responsibility of Information Security and the department responsible for the system area being assessed.

5. Roles and Responsibilities

A. Executive with Information Security responsibilities

Executive with Information Security responsibilities is responsible for:

- Leading all RA projects.
- Ensuring that the summary of all RAs is maintained.
- Approving the recommended remediation activities.

B. FileLocal

FileLocal are responsible for:

- Ensuring completeness of information supplied to staff performing RA activities.

C. Vendors

Vendors are responsible for:

- Assisting the RA staff in performing the activity.
- Implementing recommended remediation activities.
- Notifying the Executive with Information Security responsibilities in the case of a situation which would cause a change in assessment.

D. Participating Cities

Participating Cities are responsible for:

- A City's CISO, or designee, will participate in any ongoing RA activities.

6. Compliance

The Security Risk Assessment Policy uses and assimilates the following bodies of recognized knowledge:

ISO 27002:~~2005~~2013:

- Section 4 – Risk Assessment and Treatment

7. Related Documents

- PRO-310 Risk Management Process

System Development Life Cycle (SDLC)Policy (POL-130)

1. Introduction

The Washington Multi-City Business License and Tax Portal agency (FileLocal) is committed to a formalized System Development Life Cycle (SDLC) in support of its numerous publicly available software products in addition to its core data management business.

Ensuring that the SDLC includes information management and information security is a key differentiator.

2. Purpose

The purpose of System Development Life Cycle Policy is to set a minimum set of requirements which all system development projects must adhere to prior to being permitted into production use.

3. Scope

The System Development Life Cycle Policy applies to those who utilize information systems, business applications, networks and information owned by FileLocal:

- Agency staff
- Temporary supplemental staff
- Contractors
- Vendors
- Consultants
- Participating cities
- All business partners and parties

The System Development Life Cycle Policy also applies to all information systems, data, business applications and networks, used or administered by FileLocal and to all computational environments operated by, or operated on behalf of FileLocal.

Deviation from this policy is acceptable only if an information security threat and risk assessment has been completed with a documented business impact analysis and the FileLocal have signed a risk acceptance form. The Risk Acceptance Form shall be authenticated by the Program Manager.

4. Policy Statements

A. All new system development or major changes to existing systems shall consider data confidentiality, availability and integrity in its life cycle stages.

B. Systems to be developed shall be categorized, in accordance with the FileLocal Information Classification Policy, based on the level of the highest classification data component processed, inputted, outputted, stored or transmitted.

C. Risk assessments shall be performed to identify security risks of all systems to be developed, acquired or enhanced.

D. Security requirements of systems shall be identified during the specifications and design phases, prior to development and implementation.

E. All systems shall be tested thoroughly before being deployed into the production environment.

F. All production data shall be sanitized before being used as test data.

G. The software development life cycle shall adopt industry best practices and security recommendations.

H. Authentication methods shall be implemented in systems and system components to be developed or enhanced to prevent unauthorized access.

I. All user input shall be validated to prevent exploitation of input vulnerabilities.

J. Output data shall be validated to ensure that processing of data is correct.

K. Cryptographic controls shall be applied to protect data integrity and confidentiality according to the Information Classification and Encryption policies and related artifacts.

L. Major enhancement of existing systems shall be in accordance with FileLocal Documentation governance process.

M. The security specifications for system development and enhancements shall be reviewed and approved by the Executive with Information Security responsibilities.

N. All external and internal interfaces of systems to be developed or enhanced shall be documented.

O. Systems must be certified and accredited before being moved into production environment.

5. Roles and Responsibilities

A. Program Manager

The Program Manager is responsible for:

- Defining criteria used in the supporting standards.
- Reviewing design decisions.
- Providing consulting on appropriate methods.

B. FileLocal

FileLocal is responsible for:

- Ensuring projects are compliant with this policy.

C. Vendors

Vendors are responsible for:

- Implementing requirements for operations based on the SDLC design criteria. Assisting the FileLocal in understanding the implications of SDLC decisions.

D. PARTICIPATING CITIES

Participating Cities are responsible for:

- Adhering to this policy and associated standards as well as adopted Information Security polices at a City.

6. Compliance

The System Development Life Cycle Policy uses and assimilates the following bodies of recognized knowledge: ISO 27002:2013:

- Section 14.1.2 - Securing application services on public networks
- Section 12.5 – Control of operational software
- Section 14.2 – Security in Development and Support Processes

7. Related Documents

- Secure Application Development Standard

Business Continuity Policy (POL-140)

1. Introduction

Business Continuity addresses the preservation of business. In the event of disruptions caused by natural or deliberate events, it is essential that the Washington Multi-City Business License and Tax Portal Agency (FileLocal) sustain critical processes and operations in the face of business- threatening emergencies.

2. Purpose

This policy document outlines the security principles, requirements, and accountabilities for developing a Business Continuity Process for FileLocal

3. Scope

The Business Continuity Policy applies to those who utilize information systems, business applications, networks and information owned by FileLocal:

- Agency staff
- Temporary supplemental staff
- Contractors
- Vendors
- Consultants
- Participating cities
- All business partners and parties

The Business Continuity Policy also applies to all information systems, data, business applications and networks, used or administered by FileLocal and to all computational environments operated by, or operated on behalf of FileLocal.

Deviation from this policy is acceptable only if an information security threat and risk assessment has been completed with a documented business impact analysis and the FileLocal have signed a risk acceptance form. The Risk Acceptance Form shall be authenticated by the Program Manager.

4. Policy Statements

A. FileLocal shall implement a Business Continuity process to protect critical business operations and reduce disruptions to an acceptable level.

B. The Business Continuity Process shall include a combination of preventative and recovery measures.

C. Each of FileLocal business functions shall develop the necessary processes and infrastructure relevant to their aspect of the business to support the overall Business Continuity objectives.

D. The Business Continuity Plan (BCP) and supporting Activation Procedures shall include:

- Conditions for activating the BCP.

- Documenting roles, responsibilities and emergency procedures.
- Prioritizing the critical processes.
- Documenting emergency procedures to allow recovery and restoration of all critical systems
- within required times.
- Assessment of external and internal business dependencies.
- Appropriate education and training of personnel in the emergency procedures.
- Documenting required resources and equipment for the Backup Operations Center (BOC).
- Documenting procedures for recovery of operations at the BOC.
- Documenting a testing and maintenance plan to assure the reliability of backup procedures
- and systems.
- Procedures for returning to normal business operations.

5. Roles and Responsibilities

A. Program Manager

The Program Manager is responsible for:

- Identifying and determining the conditions for plan activation.
- Identifying roles and responsibilities of individuals and their alternates responsible for execution of each component of the plan.
- Developing effective communication arrangements and processes for liaison with internal and external authorities including police, fire services, government agencies and media.
- Developing a regular testing and maintenance schedule for the contingency framework.
- Conducting awareness and education activities in support of the business continuity framework.

B. FileLocal

FileLocal is responsible for:

- Developing emergency procedures.
- Developing fail-over procedures that describe actions to be taken to move critical business processes to the backup operations center and to restore business operations within the required time periods.

C. Vendors

Vendors are responsible for:

- Assisting FileLocal with developing emergency procedures.
- Assisting FileLocal with developing fail-over procedures.

- Developing procedures for restoration to normal operations.
- Identifying and reporting Business Continuity events to the Executive with Information Security responsibilities.

D. Participating Cities

Participating Cities are responsible for:

- Understanding and following the Business Continuity Policy and any further information security policies at a City.

6. Compliance

The Business Continuity Policy uses and assimilates the following bodies of recognized knowledge: ISO 27002:2013:

- Section 17 – Information Security Aspects Of Business Continuity Management

7. Related Documents

- Business Continuity Plan

Guidelines for Information Owners and Custodians

1. Introduction

These guidelines will assist the Washington Multi-City Business License and Tax Portal Agency (FileLocal) staff accountable for information assets and/or responsible for IT network operations, program development, database administration, and application system operations to understand and implement the FileLocal security standards. It is written in plain language for general dissemination and highlights the important aspects of the Security Standards.

2. Vendor Responsibilities

Kubra provides development services, and has ownership over the development process for, the mobile application provided by FileLocal, and ~~eGov~~Avenu provides tax filing services for FileLocal.

3. Owners – Asset Classification

In addition to the more traditional list of assets such as facility, land, equipment, money, and people, the list of agency assets also includes information used to support the agency. The agency's physical assets are protected because lost or damaged assets damage the agency's chances of success. In the same manner, protecting the agency's information assets enhances its chance of success. Prudent asset security yields improved value for stakeholders and improved customer service..

Information Owners are those individuals who have the final agency responsibility for information, and information system, protection. They include Data, System, Application and Network Owners and can also be the Program Manager.

Responsibilities include:

- Classification of information and information systems.
- Authorization of access rights to their data / systems / application / network.

Owners define the criticality level for assets according to the following:

- Mission critical assets (high criticality level)
- Agency critical assets (medium criticality level)
- Non-critical assets (low criticality level)

DO

- Clearly identify all assets
- Maintain an up -to -date asset inventory

A. Annual Asset inventory records should have information such as:

a. Owner
b. Type
c. Criticality
d. Version if applicable
e. Location

B. Information Classification Scheme.

There is a four-level classification scheme at FileLocal

- RESTRICTED: Compromise might result in a critical loss
- CONFIDENTIAL: Compromise might result in important or significant loss
- INTERNAL: Information that may be shared within FileLocal to users on a need-to- know basis
- PUBLIC: Information that can be shared with the public

DO

- Clearly identify the security classification of information you own, or originate, commensurate with the value of that data to FileLocal
- Maintain the classification of information you originate or own throughout its lifecycle
- Manage and communicate the creation, labelling, storage, transmittal and disposal of your information according to FileLocal requirements

A. DATA RETENTION

FileLocal is legally obligated to retain all operating records for various periods of time. Retention periods vary for different types of records and are mostly determined by statutory and regulatory requirements.

DO

- Keep all documents and data in accordance with City Of Seattle document retention guidelines.

Where the City Of Seattle guidelines do not specify a specific retention period,

- Keep terminated User information (e.g. files, e-mails) for 30 days.
- Keep Audit Trails on-line for 6 months and on secondary storage for an additional 30 months.

B. STORAGE MEDIA DISPOSAL

Data Storage Media Disposal is the process of eliminating information assets from media that is no longer required. Deleting 'RESTRICTED' and 'CONFIDENTIAL' information stored on media is not sufficient because only the file name has been removed from the directory table of contents. The information is still there until it is overwritten by new data.

The media should be rendered unreadable by a 'Secure Wiping Technique' or by the physical destruction of the media.

4. Owners – System Development

Security and functionality should be designed and developed at the same time. Developing and following a formalized Software Development Lifecycle (SDLC) process will achieve this goal. A formalized SDLC process consists the following major phases:

- Requirements definition
- Design
- Development
- Implementation
- Post-Implementation

A. Security in the Design

- Logical and physical separation of the development and production environments to ensure access to the production environment is not inadvertently granted to those with access to the development environment
- Network segregation to achieve separation of development sandbox-type systems and production systems
- Segregation of duties to achieve separation of development duties from system operational duties

DO

- Adhere to the Secure Software Design Principles
- Consider the following technical security controls be incorporated in systems:
    - Input data validation
    - Processing controls to detect errors in the processing
    - Access control
    - Logging feature
    - Cryptographic controls
- Put extra emphasis on testing systems being developed
- Adhere to the Change Control Process for adopting changes to the design

B. SECURE SOFTWARE DESIGN PRINCIPLES

When designing software systems, the following program design principles should be considered:

- **Least Privilege:** Only give users enough authorization to data to perform the required job
- **Fail Safe Defaults:** Default values for variables should enable safest, least privileged operational mode
- **Least Common Mechanism:** Anything which is shared among different programs can be a path for communication and a potential security hole, so as little data as possible should be shared
- **Economy of Mechanism:** Designs which are smaller and simpler are easier to inspect and trust
- **Complete Mediation:** Every access to every object should be checked
- **Open Design:** The application of open source methods to the creation of physical products, machines and systems
- **Separation of Privilege:** A system should ensure that multiple conditions are met before granting permissions to an object
- **Psychological Acceptability:** The system should not place an undue burden on its users

5. Custodians – Logical Access Control

A. AUTHENTICATION

Logical access controls protects systems from unauthorized access by the following means:

- **Identification:** Identifying users (e.g. based on username, account number)
- **Authentication:** Verifying ~~users'~~users identity (e.g. password, cryptographic key)
- **Authorization:** Granting access to a subject to access a system

Authentication is the security mechanism that ensures the reliable identification of the individual. Strong authentication combines of any two of the following factors

- **Type 1:** Something the user knows (i.e. password)
- **Type 2:** A physical artifact the user requires (i.e. security token)
- **Type 3:** Something unique to each user's physiology (i.e. fingerprint, voiceprint)

B. Identification

Identification of individuals is based on User IDs

DO

- Assign unique User IDs.
- Follow the naming convention for User IDs.
- Create User IDs that are at least 6 characters in length.
- Make sure that the User ID assigned to a user follows that employee throughout their employment period at FileLocal and that User IDs are not re-used.

C. Passwords

Passwords should be easy to remember but difficult to guess. Temporary passwords are permitted when:

- A new User ID is being assigned.
- A user has forgotten a password.
- A user is locked out of her/his User ID.

DO

- Configure systems to enforce strong passwords.
- Configure systems for passwords to expire after 60 days.
- Change vendor-supplied default passwords.
- Ensure passwords are not displayed on the screen or stored in clear text.
- Ensure passwords are not revealed, apart from a temporary one.
- Lock user accounts after 3 unsuccessful login attempts.

D. Authorization

Assigning access rights should be based on the following three principles:

- **Segregation of Duties:** Having more than one person required to complete a task
- **Least Privileges:** Assigning the minimum required authorization for an individual to complete a task
- **Need to Know:** Limiting access to information based on individual's role Access right are granted by Information Owners (e.g. VPs, business unit leaders)

E. REMOTE ACCESS

Allowing access from outside into the FileLocal environment exposes the following risks:

- Unauthorized access
- Interception of data during transmission

DO

- Use strong encryption and (2-factor) authentication on all remote connections
- Log all remote login access attempts
- Set a 30-minute idle timeout on the remote access server
- Document all external connections
- Display a login banner containing a warning message

6. Custodians – User Provisioning

A. User Account Creation

IS Service Desk is responsible for creating, managing and terminating user accounts.

DO

- Assign a unique ID for each user
- Ensure new User IDs are not created by cloning an existing one
- Grant an initial temporary password to the new User ID and do not leave the password blank
- Obtain a signed access rights document from the user

B. User Account Management

User accounts are changed based on Human Resource's notices about user termination or changing roles. User IDs must be verified before resetting the password.

DO

- Obtain a user update or termination notification from Human Resources before changing / deleting a user account
- Review and change access rights if a user changes roles
- Disable user accounts immediately upon user termination or departure
- Ensure Information Owners review and approve all accesses to their assets
- Positively verify a user's identity prior to resetting a password

-

C. Third Party Account Management

User accounts are changed based on Human Resource's notices about user termination or changing roles. User IDs must be verified before resetting the password.

DO

- Verify the required contractual arrangements have been completed prior to user account creation
- Grant only sufficient access to third parties required to perform their job
- Ensure Information Owners review and approve all third -party accesses to their assets
- Disable 3rd party access on the final date of the contract

7. Custodians – Infrastructure Security

A. Audit Trails

Audit trails provide accountability for the usage of FileLocal systems. Protecting the integrity of audit logs is crucial.

Audit Trails include the following information:

- Type of event
- Date and time of event
- User identification
- Origin or destination IP address of the attempt
- Identity or name of the affected data or system component or resource
- Success or failure of the activity

DO

- Enable automated log capability of systems
- Time-stamp audit trails by an accurate real time clock
- Synchronize system clocks
- Ensure classified data are not stored in the logs in clear text
- Protect the integrity and confidentiality of audit trails

B. Encryption

DO

- Use only approved encryption and hash algorithms (DES, SHA-1 and MD5 are NOT approved algorithms)
- Use only approved encryption key lengths (minimum 128 bit for AES, 112 ~~bits~~bit for 3DES and 1024 for RSA)
- Transmit and store classified information (RESTRICTED and CONFIDENTIAL) in encrypted form

- Protect cryptographic keys during the life-cycle of the key from modification, destruction and unauthorized disclosure
- Change symmetric cryptographic keys on a 6-month basis

C. Infrastructure Security in Networks / Servers / Desktops

Networks consist of devices such as firewalls, IDS/IPS, routers, switches, VPN concentrators.

DO

- Backup device configuration files regularly
- Apply security patches and updates regularly
- Use encrypted connections for remote administration
- Disable clear text protocols
- Ensure changes follow the Change Management Process
- Change vendor default settings immediately
- Ensure devices provide logs on security events / access attempts
- Document device configurations
- Harden all systems to a baseline standard prior to deployment in the FileLocal infrastructure
- Ensure network incidents are recorded, review and resolved
- Disable web services running on the routers/switches
- Present users with warning banners at login
- Delete data securely when systems are decommissioned or retired

D. Infrastructure Security in Wireless LAN

Wireless communication technologies, also referred to as WLAN, consist of the following technologies:

- ~~Wi-Fi~~802.11x
- Infrared
- Bluetooth
- RF Wireless keyboard

Due to the lack of inherent security features, only WiFi 802.11x is permitted to be used on FileLocal premises~~:~~

.

DO

- Use WiFi Protected Access (WPA) instead of Wireless Equivalency Protocol (WEP)
- Disable SSID broadcast
- Use 128-bit encryption
- Use 802.1X port authentication
- Apply a strong authentication method, such as two-factor authentication
- Perform secure device authentication
- All vendor default settings are changed
- Disable access to reported stolen WLAN devices immediately
- Apply security patches for WLAN devices regularly
- Use encrypted connections for remote administration
- Enable logging on WLAN access points
- Perform a site survey prior to deploying a WLAN

DO NOT

- Allow ad hoc connections between stations

8. Custodians – Application, System and Network Operational Security

A. Patch Management

Patch management is performed according to the formal patch management process.

DO

- Obtain security patches from reputable sources
- Apply patches according to the Change Management Process
- Test security patches before deploying
- Ensure a rollback strategy is in place before applying patches
- Backup systems prior to the installation of new patches
- Apply automatic software updates and deployment when applicable
- Document installed patches including at minimum:
    - Name of the device
    - Name of the patch
    - Version of the patch
    - Date of installation
    - Name of the person who installed the patch
    - Any problems encountered

B. DATA BACKUP

DO

- Retain backup data according to Data Retention requirements
- Handle backups with the same care as the data stored on them
- Test backups, restore procedures and equipment regularly
- Transport backups in a secure manner and maintain off-site backups in a secure location

E. Malicious Attacks

There are several types of malicious threats to FileLocal personnel, data and systems. Past viral attacks were designed to damage or disrupt a system. Today's malicious code is designed to silently steal data for profit without doing noticeable damage that would alert the user to its presence.

DO

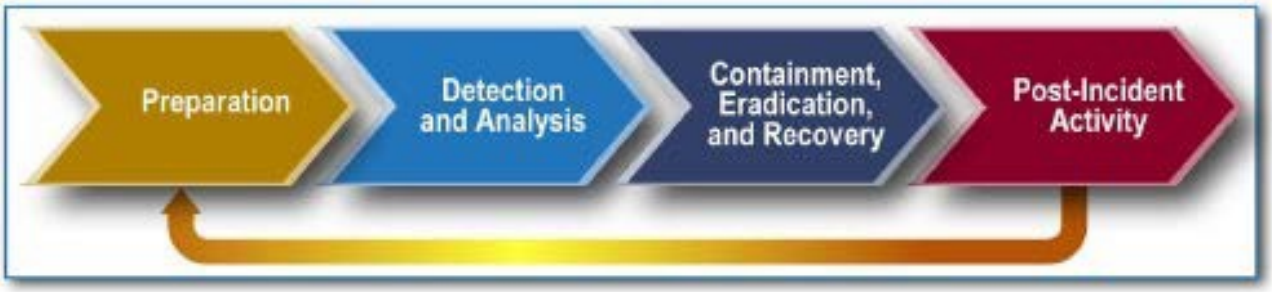
- Centrally manage and monitor antivirus products
- Ensure Antivirus software cannot be disabled on end user computers
- Apply antivirus software at email gateway
- Ensure antivirus software generates audit logs
- Update virus definitions automatically and regularly

9. Custodians – Physical Security

DO

- Obtain security clearance requests from Owners prior to granting access to FileLocal facilities.
- Maintain physical access logs for 3 months
- Physically secure publicly accessible network access points
    - Close blinds in restricted ~~areas~~
- area

10. Custodians – Responding to Security Incidents



When detected, there must be a structured response to security incidents so that the incident is dealt with quickly and comprehensively and forensic evidence can be collected if necessary. There are six stages to a structured security incident response:

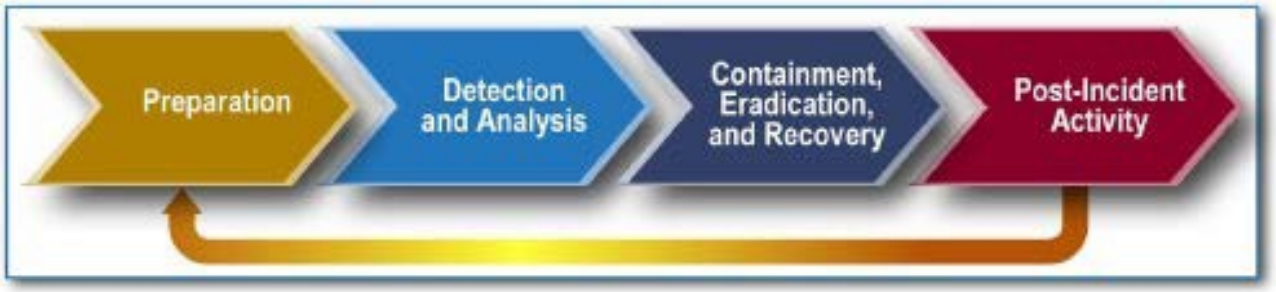


Figure 1- Security Incident Response Process

- Preparation: This phase will be critical to ensuring that all other phases are performed adequately
- Detection and Analysis: This is the ability to identify incidents
- Containment: This isolates the systems affected by the incident
- Eradication: This removes the cause of the incident, for example deleting a virus
- Recovery: This restores and returns the system to operational status
- Post-Incident Activity: This is the investigation into the initial cause of the incident

DO

- Establish a Computer Security Incident Response Team (CSIRT) that responds to incidents
- Develop a structured incident response process
- Ensure FileLocal management is involved when rising incident severity warrants escalation
- Train and exercise CSIRT members in the incident response process
- Integrate Intrusion Detection System (IDS) and Security Incident and Event Management (SIEM) system with incident response process and IT operations
- Educate Service Desk personnel in incident detection techniques and incident escalation

- Collect and record information as an incident investigation evolves, including:
  - Current status of the incident
  - Actions taken during the Security Incident response
  - Actions taken by Security Investigators for each incident
  - A list of the evidence gathered during the incident investigation / analysis phase
  - Comments and notes 'to-file' or in any form from Security Investigators
  - Planned Steps to be started in a Security Investigation

11. Asset Inventory

11.1 Introduction

This inventory is intended as a reference for FileLocal to use to track all FileLocal information assets (servers, laptops, etc.) and should be updated on at least an annual basis, or following any significant changes to FileLocal's operating environment.

11.2 Inventory

Asset Name (fully qualified	Location	Description/Purpose (including criticality	Party Responsible/Owner	Serial Number

For further details on any statement in this guide, please refer to the related policy or standard or ask your manager or information security representative.

Public Records Policy

1. PURPOSE

   A. The purpose of this policy is to define public records and provide a procedure for the proper reporting and response to records requests.

   B. The Revised Code of Washington (RCW) ~~42.56,~~42.56, commonly known as the Public Records Act, requires public agencies to make identifiable, non-exempt public records available for inspection and copying upon request and to publish rules of procedure to inform the public how access to public records will be accomplished.

   C. In carrying out its responsibilities under the Act, FileLocal will be guided by the provisions of the Public Records Act describing its purposes and interpretation.

2. RESPONSIBILITY

   A. FileLocal's Program Manager and designated Public Records Officer

3. BACKGROUND

   A. FileLocal public records are available for public inspection and duplication, except as otherwise provided by RCW ~~42.56.001-42.56.904~~ 42.56.001-42.56.904 or other statutes. All records will be released if they do not fall within the specific exemptions of the Public Records Act or other statutes which exempt or prohibit disclosure of specific information or records.

   B. The Public Records Act defines a public record as any "writing containing information relating to the conduct of government or the performance of any governmental or proprietary function prepared, owned, used or retained" by the agency.

   C. "Writing," broadly defined, means "handwriting, typewriting, printing, Photostatting, photographing, and every other means of recording any form of communication or representation, including, but not limited to, letters, words, pictures, sounds, or symbols, or combination thereof, and all papers, maps, magnetic or paper tapes, photographic films and prints, motion picture, film and video recordings, magnetic or punched cards, discs, drums, diskettes, sound recordings, and other documents including existing data compilations from which information may be obtained or translated." This includes emails, text messages, blogs, tweets and any emerging technologies used to conduct agency business.

   D. FileLocal makes many public records available on its website:FileLocal.org

   E. Original FileLocal records will not be permitted out of the FileLocal premises. Inspection of any public records shall be conducted in the presence of a Public Records Officer or designee. No public record may be marked, defaced, torn, damaged, destroyed, unreasonably disorganized, or removed from its proper location by order of a member of the public.

4. FILELOCAL PROCEDURES

   A. FileLocal's business office is located at 700 5th Avenue, Suite 4350. Seattle WA 98124.

   B. The FileLocal Public Records Officer is the Program Manager.

   C. All requests for public records must be directed in writing to the Public Records Officer and should specify that they are a request for public records under the state public records act. A public records request form will be provided on the FileLocal website.

   D. A set per-page charge of $0.15 will be assessed for 10 or more pages of black and white copies of letter or legal-sized pages (each side of a sheet is one page). If FileLocal has to pay an outside firm for duplicating records in non-routine formats such as photographs, blueprints or tape recordings, the actual costs will be passed along to the requestor.

   E. Before beginning to copy records, the Public Records Officer or designee may require a deposit of up to ten percent of the estimated costs of copying the records selected by a requestor. The Public Records Officer may also require the payment of the remainder of the copying costs before providing all of the records, or the payment of the costs of copying an installment before providing that installment. Payment may be made by check or money order to FileLocal.

   F. The Public Records Officer has the discretion to waive copying charges for small requests or for individuals or government agencies doing business with FileLocal if the Public Records Officer determines that this action is in the best interest of the agency.

   G. If possible, electronic records should be provided in their existing format, if requested in that format. However, if it necessary to burn files to a device the requestor may be charged $1.00 per CD or $10 per 16 GB thumb drive. When standard 8 ½ x 11 records are scanned from paper to .pdf, the requestor may be charged .10 cents per page.

5. RECORDS EXEMPT FROM DISCLOSURE

   A. After FileLocal has gathered responsive records, FileLocal will determine whether an exemption applies to all or part of the record.

   B. FileLocal is not required to permit public inspection and copying of records for which public disclosure of the record is prohibited or limited by state or federal statue or regulation. If any item is withheld, a written statement of the specific reasons will be provided by the Public Records Officer.

6. DELETION/REDACTION OF EXEMPT MATERIALS

   A. FileLocal is not relieved of its obligation to respond to requests for public records because a portion of the record contains information covered by an exemption. FileLocal has a duty to delete or redact specific information covered by an exemption and disclose the remainder of the record.

   B. If any item is withheld, a written statement of the specific reasons will be provided by the Public Records Officer.

7. MAKING A PUBLIC RECORDS REQUEST

   A. Contact information for FileLocal's Public Records Officer and procedures for making a public disclosure request are to be clearly identified on the FileLocal website – including the provision of an online form and/or PDF.

B. Requestors are encouraged to view the many documents available on the FileLocal website (www.filelocal.org) prior to submitting a public records request.

C. Any person wishing to request access to public records or seeking assistance making a request should contact FileLocal's public records officer. The Public Records Officer oversees compliance with the Public Records Act but may designate other staff who may process requests of public records.

D. The Public Records Officer may be reached at 700 5th Avenue, Suite 4350; P.O. Box 94669; Seattle WA 98124-4669; Jamie-Carnell (Jamie.Carnell-FLO@seattlle.gov) or phone 206-615-0493.

E. Persons making a public records request should include the following information, in writing:

I. Date and time of the request

II. Name of requestor

III. Contact information for the requestor

IV. Date range for the records requested

V. A detailed description of the requested records including the document name, if applicable.

8. PROCESSING OF PUBLIC RECORDS REQUESTS

A. Within five (5) business days from the receipt of the request, FileLocal must respond by:

I. Making the records available for inspection or copying; **OR**

II. If copies are requested and payment has been received, sending the copies to the requestor; **OR**

III. Acknowledgement of the receipt of the request and an estimate of additional time needed to produce the information requested; Additional time required to respond to a request may be based on the need to clarify the intent of the request, to locate and assemble information requested, to notify third persons or agencies affected by the request, or to determine whether any of the information requested is except and that a denial should be made to all or part of the request; **OR**

IV. Denial of the request and providing a written statement of specific reasons.

B. If FileLocal does not respond in writing within five business days of receipt of the request for disclosure, the requestor should consider contacting the Public Records Officer to determine the reason for the failure to respond.

C. When a records request is for a large volume of records, FileLocal may elect to provide the records on an installment basis.

9. RECORDS INSPECTION

A. Public records are available for inspection and copying during normal business hours (Monday through Friday 10 a.m. to 2 p.m., excluding legal holidays). The agency and requestor can make mutually agreeable arrangements for times of inspection and copying. Records must be inspected at the FileLocal offices.

B. FileLocal will maintain its records in a reasonably organized manner and will take reasonable actions to protect records from damage and disorganization. A requestor shall not take FileLocal records from the agency offices without the permission of the Public Records Officer or designee.

10. RECORDS INDEX

A. Compliance with RCW ~~42.17.260(3)~~ 42.17.260(3) is unnecessary, would be unduly burdensome and would interfere with FileLocal's implementation of an efficient, cost-effective business license and tax portal. The maintenance of detailed indexes is not practical or feasible and cannot be accomplished within the project schedule and budget because of limited staff resources, the voluminous ~~number~~amount of documents associated with the project, and the contract management approach to project development and operations.

11. RETENTION OF RECORDS

A. FileLocal is not required to retain all records it creates or uses. Retention schedules vary based on the content of the record. FileLocal will retain records in accordance with retention schedules approved by the State Local Records Committee. Public records may not be destroyed per a retention schedule if a public records request or actual or anticipated litigation is pending.

B. Because an electronic record is usually more susceptible to manipulation and alteration than a paper record, FileLocal will keep, when feasible, an electronic copy of the electronic records it provides to a requestor to be able to show the exact records it provided if necessary

C. FileLocal's records will be stored in a safe, secure, and accessible manner. Documents and financial files that are essential to keeping FileLocal operating in an emergency will be duplicated or backed up at least every week and maintained off-site.

D. FileLocal's Secretary is responsible for the ongoing process of identifying its records, which have met the required retention period, and overseeing their destruction. Destruction of financial and personnel-related documents will be accomplished by shredding.

E. Personal electronic devices, if used to conduct FileLocal business, will be subject to public disclosure. Failure on the part of employees to follow this policy can result in possible civil and criminal sanctions against FileLocal and its employees and possible disciplinary action against responsible individuals.

F. FileLocal's Program Manager will periodically review these procedures with FileLocal's legal counsel and certified public accountant to ensure that they are in compliance with new or revised regulations.

12. PUBLIC DISCLOSURE LOG

A. The FileLocal Public Disclosure Officer will maintain a log of all public disclosure requests including: tracking staff time and expenditures related to the responses to records requests and the request date, response date, closing date, requestor name, responsible parties, referrals to other departments, general subject of request, general information on redactions, and information on appeals and determinations.

13. PUBLIC DISCLOSURE TRAINING

    A. Training has been and will continue to be provided to all FileLocal Executive Board members and staff to create a culture of compliance within the organization.

14. DISCLAIMER OF LIABILITY

    A. This policy is not intended to expand or restrict the rights of disclosure of privacy as they exist under state and deferral law. Despite the use of any mandatory terms such as “shall” nothing in this policy is intended to impose mandatory duties on FileLocal beyond those imposed by the state and federal law.

15. ANNUAL REVIEW OF POLICIES BY EXECUTIVE BOARD

- The FileLocal Program Manager will review these policies on an annual basis

Use of Electronic Signatures

1. PURPOSE

To ~~detail the~~ establish an electronic signature policy for FileLocal, under the authority of Section 18, Engrossed Substitute Senate Bill 6028, Chapter 57, Laws of 2020 (repealing and ~~procedures for control of~~ replacing Chapter 19.360 RCW), that:

- Promotes electronic transactions and removes barriers to conducting electronic transactions;
- Promotes efficiency in order to conserve public resources;
- Establishes guidelines for the use of electronic signatures for certain agency records and transactions;
- Controls the process for applying or obtaining signatures on agency resolutions and business ~~correspondence and provide general direction on ensuring the~~ records;
- Provides reasonable assurance of the integrity, authenticity, ~~integrity,~~ and nonrepudiation of documents when signed using electronic signatures; and
- Determines the scope of use of the current electronic signature platform provider (Adobe Sign) as the approved method for affixing an electronic signature to an electronic record. These policies will apply to any future replacement of the Adobe Sign platform.

Additionally, reducing FileLocal's reliance on paper-based transactions will further improve information security~~, and accessibility of e-records including those that are electronically signed~~ and sharing, allow faster approval of and access to documents, and reduce costs and environmental impacts.

~~1. POLICY~~

2. DEFINITIONS

Authentication: The assurance that the electronic signature is that of the person purporting to sign the record or conduct the electronic transaction.

Electronic ~~signatures will be allowed for the officers~~record: A record created, generated, sent, communicated, received, or stored by electronic means.

Electronic signature: An electronic sound, symbol, or process attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to authenticate or adopt the record.

Record: Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form, except as

otherwise defined for the purpose of state or local agency record retention, preservation, or disclosure.

Sign: With present intent to adopt or authenticate a record, to execute or adopt a tangible symbol, or to attach to or logically associate with a record an electronic symbol, sound, or process.

Tangible medium: A writing, copy of a writing, facsimile, or a physical reproduction, each on paper or on other tangible material.

Wet Signature: A signature created when a person physically marks a document with a name or symbol, using a pen, seal, or similar writing instrument, with the intent to adopt or authenticate the record.

3. POLICY

A. An Electronic Signatures Recognized. FileLocal encourages electronic transactions and the use of electronic signatures. Filelocal recognizes electronic signatures as legally binding and equivalent in force and effect as wet signatures and authorizes the use and acceptance of electronic signatures as a substitute for wet signatures on agency records requiring or allowing signatures, except as provided herein or as otherwise required by law.

~~A.~~B. Persons Authorized to Use Electronic Signatures. The Program Manager, Chair and Vice Chair of the Executive Board ~~subject to the security procedures described below~~, and their designees ("Authorized Persons") are authorized to sign agency records using any electronic signature platform approved under this policy to affix their electronic signatures to agency records as provided in this policy.

~~1. RESPONSIBILITY~~

~~Program Manager~~

~~1. PROCEDURE~~

C. ~~An~~Adobe Sign Authorized. The Adobe Sign electronic ~~version~~signature platform, and any future replacement of ~~resolutions~~the Adobe Sign platform, is hereby approved and authorized for use in affixing electronic signatures of Authorized Persons to all agency records for which an electronic signature is required or permitted under this policy.

D. Desired-Signature Transactions: Electronic signatures may be used when a valid written or electronic signature is not required by ~~the~~ law, regulation, or agency policy but is desired to emphasize the significance or importance of a record or transaction ("Desired-Signature Transactions"). In these cases, there is no legal requirement for authentication, and a signature method other than Adobe Sign is authorized (i.e. use of digital image of signature). Examples of Desired-Signature Transactions include, but are not limited to, memos, correspondence, meeting minutes, time sheets, and approved

claims vouchers. Adobe Sign or a wet signature may be used for such documents, but it is not required.

E. Required-Signature Transactions: Electronic signatures may be used by Authorized Persons when law, regulation, or agency policy requires a record or transaction to have a valid signature before it is considered legally effective ("Required-Signature Transactions"). Required-Signature Transactions include, but are not limited to, contracts, offer letters, and Executive Board ~~shall be~~ resolutions. In these cases, the signature method must be Adobe Sign, or a replacement platform that is equally capable of secure authentication of the signer.

F. Executive Board Resolutions: For resolutions approved by the Executive Board, an electronic copy of the resolution will be provided by the Program Manager ~~to the signature authority such~~ or designee to the authorized signatory for that person to sign. For electronic signatures, the authorized signatory shall sign the resolution as ~~the chair, vice, chair, secretary, and/or treasurer as appropriate for the document to be signed.~~a Required-Signature Transaction under this policy and return it to the Program Manager or designee for retention.

~~B. The signature authority shall sign in blue ink a printout of the document and return a scanned version of the signed document to the Program Manager along with an email stating that the attached document is signed and approved.~~

G. ~~The signature authority may also send an email to the Program Manager stating in writing that the~~ Wet Signatures Authorized. This policy in no way affects FileLocal's ability to sign a record or conduct a transaction using a physical medium and shall not be construed as a prohibition on the use of wet signatures.

H. Changes to this Policy. This policy may be amended, rescinded, or replaced at any time by the Executive Board, except that the Program Manager is authorized to substitute a different electronic signature platform that, in his or her discretion, has equal or better security, integrity, and auditability features as Adobe Sign.

~~A. Program Manager is authorized to sign for the Executive Board member.~~

~~B. Guidelines for the retention and preservation of electronically signed records, including maintaining the attachment or logical association between the signed record and signature, will be addressed separately in the policy on public records.~~

KEY GOVERNANCE DOCUMENTATION

The Washington Multi-City Business License and Tax Portal (dba FileLocal) was formed in March 2014 under an Interlocal Agreement and Related Articles of Incorporation.

The agency is organized as a public body and instrumentality of its members to jointly exercise essential governmental functions of its members in accordance with the Interlocal Cooperation Act (39.34 RCW), which permits a local government to enter into interlocal agreements with other public agencies in the interest of cooperatively sharing resources for their mutual benefit.

FileLocal's Articles of Incorporation are filed with the Washington Secretary of State and are the primary rules governing the management of the enterprise. Key documentation included in Appendix A:

1. Articles of Incorporation
2. Interlocal Agreement
3. Bylaws



ARTICLES OF INCORPORATION

5. APPENDIX NO. A1

ARTICLES OF

INCORPORATION OF

WASHINGTON MULTI-CITY BUSINESS LICENSE AND TAX PORTAL AGENCY

The undersigned, in order to form a not for profit corporation under Chapter 24.06 of the Revised Code of Washington ("RCW"), and pursuant to Chapter 39.34 RCW, hereby sign and deliver the following Articles of Incorporation:

ARTICLE I — NAME

The name of this corporation is:

WASHINGTON MULTI-CITY BUSINESS LICENSE AND TAX PORTAL AGENCY

ARTICLE II — DURATION

The period of duration of Washington Multi-City Business License and Tax Portal Agency (the "PORTAL AGENCY") is perpetual.

ARTICLE III — PURPOSES

PORTAL AGENCY is organized on behalf of and as an instrumentality of its governmental members to carry out certain exclusively governmental activities and the purposes of the Washington Multi-City Business License and Tax Portal Agency Interlocal Agreement (the "Interlocal Agreement") pursuant to the Interlocal Cooperation Act, Chapter 39.34 RCW. These purposes include developing, owning, operating and managing and maintaining an internet web application gateway to administer City business licensing and tax collection functions (the "Portal"), as further described in the Interlocal Agreement.

ARTICLE IV — PROHIBITED ACTIVITY

Notwithstanding any of the provisions of these Articles of Incorporation, the PORTAL AGENCY shall not conduct or carry on activities not permitted to be conducted or carried on by an organization exempt from federal income tax under Sections 115 of the Internal Revenue Code or by an organization, contributions to which are deductible under Section 170(c)(2). No part of the net earnings of the PORTAL AGENCY shall inure to the benefit of any director,

officer or private individual. No substantial part of the activities of the PORTAL AGENCY shall be devoted to the carrying on of propaganda, or otherwise attempting to influence legislation except as may be permitted by the Internal Revenue Code, and the PORTAL AGENCY shall not participate in, or intervene in (including the publication or distribution of statements regarding) any political campaign on behalf of or in opposition to any candidate for public office. The PORTAL AGENCY

shall not have or issue shares of stock, shall not make any disbursement of income to its directors or officers, and shall not make loans to its officers or directors.

ARTICLE V — POWERS

In general, and subject to such limitations and conditions as are or may be prescribed by law, or in these Articles of Incorporation or in the PORTAL AGENCY'S Bylaws or in the Interlocal Agreement, the PORTAL AGENCY shall have all powers which now or hereafter are conferred under Chapters 24.06 and 39.34 RCW and other applicable law upon a corporation organized for the purposes set forth above, or are necessary or incidental to the powers so conferred, or are conducive to the attainment of the PORTAL AGENCY's purposes.

ARTICLE VI — MEMBERS

Each Member of PORTAL AGENCY must be a general-purpose municipal corporation formed and existing as a city or town under the laws of the state of Washington and meeting the other requirements described in the Interlocal Agreement. As used in these Articles, the term "Members" means "Principals" as defined in the Interlocal Agreement. The rights and responsibilities of the Members/Principals and the manner of their election, appointment, or admission to membership and termination of membership shall be as provided for in the Interlocal Agreement. The PORTAL AGENCY shall have one class of Members/Principals, except that each Member/Principal may be treated as a separate class for calculating votes as provided for in the Interlocal Agreement.

ARTICLE VII — DISTRIBUTIONS UPON DISSOLUTION

No director, trustee or officer of the PORTAL AGENCY, nor any private individual, shall be entitled to share in the distribution of any of the corporate assets upon dissolution of the PORTAL AGENCY or the winding up of its affairs. Upon dissolution of the PORTAL AGENCY, after paying, satisfying, and discharging, or making adequate provision therefor, of all liabilities and obligations of the PORTAL AGENCY, and after returning, transferring, or conveying assets held by the PORTAL AGENCY requiring return, transfer, or conveyance on condition of the dissolution, all remaining assets of the PORTAL AGENCY shall be distributed by the Executive Board as provided for in the Interlocal Agreement.

ARTICLE VIII — DISSENTING MEMBERS

"Dissenting members," as that term is used in RCW 24.06.245 through 255, will be entitled to the rights and allocation of assets set forth in the Interlocal Agreement, but may be limited to "a return of less than the fair value" of their membership as that term is used in RCW 24.06.255.

ARTICLE IX — BYLAWS

Provisions for the regulation of the internal affairs of the PORTAL AGENCY shall be set forth in the Bylaws of the PORTAL AGENCY.

ARTICLE X — REGISTERED AGENT

The address of the initial registered office of the PORTAL AGENCY is 600 4th Avenue Seattle WA 98104. The name and address of its initial registered agent is Glen Lee, Finance Director, City of Seattle, 700 Fifth Avenue, Suite 4350, Seattle, WA 98104.

ARTICLE XI — DIRECTORS

The initial board of directors (referred to in the Interlocal Agreement as the "Executive Board") shall consist of four (4) directors. The names and addresses of the persons who are to serve as initial directors are:

Ms. Jan Hawn, Finance Director
City of Bellevue
450 110th Avenue N.E.
Bellevue, WA 98004

Ms. Debra Bryant, Chief Finance Director
City of Everett
2930 Wetmore Avenue
Everett, WA 98201

Mr. Glen Lee, Finance Director
City of Seattle
700 Fifth Avenue, Suite 4350
Seattle, WA 98104

Mr. Andy Cherullo, Finance Director
City of Tacoma
747 Market Street
Tacoma, WA 98402

Directors may be removed as provided for in the Bylaws.

ARTICLE XII -- OFFICERS

The PORTAL AGENCY shall have four officers, a President, Vice-President, Secretary and

Treasurer. The President and Vice-President are referred to as the "Chair" and Vice-Chair" respectively, in the Interlocal Agreement. The responsibilities of the officers shall be described in the PORTAL AGENCY Bylaws.

ARTICLE XIII — INCORPORATORS

The names and addresses of the incorporators are:

1. City of Bellevue
   450 110th Avenue N.E.
   Bellevue, WA 98004

2. City of Everett
   2930 Wetmore Avenue
   Everett, WA 98201

3. The City of Seattle
   600 4th Avenue
   Seattle, WA
   98104

4. City of Tacoma
   747 Market Street
   Tacoma, WA
   98402

ARTICLE XIV — LIMITATION OF DIRECTOR LIABILITY

Except to the extent otherwise required by applicable law (as it exists on the date of the adoption of this Article or may be amended from time to time), a director of the PORTAL AGENCY (a director is referred to as a "Member of the Executive Board" in the Interlocal Agreement) shall not be personally liable to the PORTAL AGENCY for monetary damages for conduct as a director, except for liability of the director (i) for acts or omissions which involve intentional misconduct by the director or a knowing violation of law by the director, (ii) for any transaction from which the director will personally receive a benefit in money, property or services to which the director is not legally entitled, or (iii) for any act or omission occurring before the date when this provision becomes effective.

If the Washington Nonprofit Miscellaneous and Mutual Corporation Act (the "Act") ~~is~~I hereafter amended to expand or increase the power of the PORTAL AGENCY to eliminate or limit the personal liability of directors, then, without any further requirement of action by the directors of the PORTAL AGENCY, the liability of a director shall be eliminated or limited to the full extent permitted by the Act. No amendment to or repeal of this Article shall adversely affect any right of protection of any director of the PORTAL AGENCY occurring after the date of the adoption of this Article and prior to such amendment or repeal.

ARTICLE XV — INDEMNIFICATION

Except as provided in Article XIV, the PORTAL AGENCY shall indemnify any director and officer of the PORTAL AGENCY who is involved in any capacity in a proceeding (as defined in RCW 23B.08.500, as presently in effect and as hereafter amended) by reason of the position held by such person or entity in the PORTAL AGENCY to the full extent allowed by law, as presently in effect and as hereafter amended. By means of a resolution or of a contract specifically approved by the Board of Directors (referred to as the "Executive Board" in the Interlocal Agreement), the PORTAL AGENCY may also indemnify an employee, or agent to such degree as the Board of Directors determines to be reasonable, appropriate, and consistent with applicable law and to be in the best interests of the PORTAL AGENCY. Reasonable expenses incurred by a director or officer who is involved in any capacity in a proceeding by reason of the position held in the PORTAL AGENCY, shall be advanced by the PORTAL AGENCY to the full extent allowed by and on the conditions required by applicable law, as presently in effect and as hereafter amended.

The Board of Directors of the PORTAL AGENCY shall have the right to designate the counsel who shall defend any person or entity who may be entitled to indemnification, to approve any settlement, and to approve in advance any expense. The rights conferred by or pursuant to this Article shall not be exclusive of any other rights that any person may have or acquire under any applicable law (as presently in effect and as hereafter amended), these Articles of Incorporation, the bylaws of the PORTAL AGENCY, a vote of the Board of Directors of the PORTAL AGENCY, or otherwise. No amendment to or repeal of this Article shall adversely affect any right of any director, officer, employee, or agent for events occurring after the date of the adoption of this Article and prior to such amendment or repeal.

The PORTAL AGENCY shall also indemnify and hold harmless every Member/Principal, including, but not limited to that Member's/Principal's officers, directors, employees and agents from all claims, injuries, damages, losses or suits, including reasonable attorney fees which arise out of acts and/or omissions of the PORTAL AGENCY. To such degree as the board of directors/Executive Board determines to be reasonable, appropriate, and consistent with applicable law and to be in the best interests of the PORTAL AGENCY, the PORTAL AGENCY may also indemnify and hold harmless Subscribers, including, but not limited to that Subscriber's officers, directors, employees and agents from all claims, injuries damages, losses or suits, including reasonable attorney fees which arise out of acts and/or omissions of the PORTAL AGENCY.

Nothing in these Articles of Incorporation may be interpreted as a waiver of sovereign immunity by any member.

Indemnification of directors and officers by the PORTAL AGENCY shall be consistent with the terms of the Interlocal Agreement, the Act, the Interlocal Cooperation Act and other applicable Jaw. In the event of any inconsistency between this Article and the Interlocal Agreement, the terms of the Interlocal Agreement shall control to the extent consistent with applicable law.

Notwithstanding any other provision of this Article, no indemnification shall be provided to any person if in the reasonable opinion of competent counsel, payment of such indemnification would cause the PORTAL AGENCY to lose its exemption from federal income taxation.

DATED as of this 1st day of March 2014.

INCORPORATORS:

INCORPORATOR: City of Bellevue



By: Interim City Manager Brad Miyake

INCORPORATOR: The City of Seattle

_____

by: Mayor Edward B. Mu1Tay

INCORPORATOR: City of Everett

_____

By: Mayor Ray Stephanson

INCORPORATOR: City of Tacoma

_____

by: City Manager T.C. Broadnax

Indemnification of directors and officers by the PORTAL AGENCY shall be consistent with the terms of the lnterlocal Agreement, the Act, the Interlocal Cooperation Act and other applicable law. In the event of any inconsistency between this Article and the lnterlocal Agreement, the terms of the Interlocal Agreement shall control to the extent consistent with applicable law.

Notwithstanding any other provision of this Article, no indemnification shall be provided to any person if in the reasonable opinion of competent counsel, payment of such indemnification would cause the PORTAL AGENCY to lose its exemption from federal income taxation.

DATED as of this 1st day of March 2014.

INCORPORATORS:

INCORPORATOR: City of Bellevue

By: Interim City Manager Brad Miyake

INCORPORATOR: The City of Seattle

by: Mayor Edward B. Murray

INCORPORATOR: City of Everett

By: Mayor Ray Stephanson

ATTEST:

City Clerk

INCORPORATOR: City of Tacoma

By: City Manager T.C. Broadnax

Indemnification of directors and officers by the PORTAL AGENCY shall be consistent with the tem1s of the Interlocal Agreement, the Act, the Interlocal Cooperation Act and other applicable law. In the event of any inconsistency y between this Article and the Interlocal Agreement, the terms of the Interlocal Agreement shall control to the extent consistent with applicable Jaw.

Notwithstanding any other provision of this Article, no indemnification shall be provided to any person if in the reasonable opinion of competent counsel, payment of such indemnification would cause the PORTAL AGENCY to lose its exemption from federal income taxation.

DATED as of this 1st day of March 2014.

JNCORPORATORS:

JNCORPORATOR: City of Bellevue

By: Interim City Manager Brad Miyake

INCORPORATOR: The City of Seattle

By: Mayor Edward B. Murray

INCORPORATOR: City of Everett

By: Mayor Ray Stephenson

INCORPORATOR: City of Tacoma

by: City Manager T.C. Broadnax

Indemnification of directors and officers by the PORTAL AGENCY shall be consistent with the terms of the Interlocal Agreement, the Act, the Interlocal Cooperation Act and other applicable law. In the event of any inconsistency between this Article and the Interlocal Agreement, the terms of the Interlocal Agreement shall control to the extent consistent with applicable law.

Notwithstanding any other provision of this Article, no indemnification shall be provided to any person if in the reasonable opinion of competent counsel, payment of such indemnification would cause the PORTAL AGENCY to lose its exemption from federal income taxation.

DATED as of this 1st day of March 2014.

INCORPORATORS:

INCORPORATOR: City of Bellevue

By: Interim City Manager Brad Miyake

INCORPORATOR: The City of Seattle

by: Mayor Edward B. Munday

INCORPORATOR: City of Everett

By: Mayor Ray Stephenson

INCORPORATOR: City of Tacoma

By: City Manager T.C. Broadnax



INTERLOCAL AGREEMENT

6. APPENDIX NO. A2

WASHINGTON MULTI-CITY BUSINESS LICENSE AND TAX PORTAL AGENCY INTERLOCAL AGREEMENT

BY AND BETWEEN THE CITIES OF

BELLEVUE

EVERETT

SEATTLE

and

TACOMA

DATED AS OF MARCH 1, 2014

TABLE OF CONTENTS

Section	Caption	Page
	Recitals……	1
1	Creation of Washington Multi-City Business License and Tax Portal Agency….	2
2	Term of Agreement……	2
3	Definitions……....	3
4	Guiding Principles and Goals…….	6
5	Portal Agency Services……...	8
6	Portal Agency Powers…….	10
7	Executive Board: Composition and Operation……...	11
8	Conversion of Status of Participating Cites; Addition of New Principals or Subscribers……..	15
9	Tax and Finance Operations Committee…….	16
10	Portal Agency Staffing……	17
11	Portal Agency Manager……...	18
12	Assignment of Portal Services Contract from Seattle to Portal Agency……	19
13	Budget; Cost Allocation; Capital Cost Recovery Charges; Payment of Charges; Delinquencies; Reserve Funds……	19
14	Retained Authority and Responsibility of Participating Agencies…….	23
15	Ownership of Property……	23
16	Merger or Consolidation, or Sale of All or Substantially All Assets……..	24
17	Withdrawal by, or Termination of, a Principal……...	24
18	Amendment of Agreement…….	25
19	Termination of Agreement; Dissolution of Agency……	25
20	Dispute Resolution……..	26
21	Insurance……	27
22	Indemnification and Hold Harmless……...	27
23	Intergovernmental Cooperation……..	28
24	Notice……..	29
24	Venue……..	29
26	Filing……...	29
27	No Third-Party Beneficiaries……..	29
28	Severability…….	30
29	Ratification……..	30
30	Execution, Counterparts and Effective Date……...	30
	List of Exhibits……...	32
A	Proposed 2014 Portal Agency Budget Summary……..……...	33
B	2015-2020 Estimated Portal Agency Operating Budget Summary……	35
C	Capital Cost Recovery Charges…….....	37
D	Calculation of New Participant Capped Cost Increment and New Participant Labor Cost Increment……...	38

WASHINGTON MULTI-CITY BUSINESS LICENSE AND TAX PORTAL AGENCY INTERLOCAL AGREEMENT

THIS AGREEMENT, incorporating all exhibits hereto, is entered into by and between the Cities of Bellevue, Everett, Seattle and Tacoma (collectively, the "Principals") pursuant to the Interlocal Cooperation Act Ch. 39.34 RCW and has been authorized by the legislative body of each Principal.

RECITALS

WHEREAS, each of the Principals is a city, a general-purpose municipal corporation authorized by state law to issue local business licenses and collect a variety of local taxes; and

WHEREAS, the Principals seek to make it easier and more efficient for businesses to apply for local business licenses and file local taxes, while retaining local control over local licensing and tax collection functions and policies; and

WHEREAS, the Principals seek to accomplish these goals by jointly facilitating the creation of an internet web application gateway (the "Portal") where tax collection and business licensing functions can be collectively administered, and where businesses operating in multiple cities can use a "one-stop" system for tax payment or business license application filing; and

WHEREAS, the Principals have engaged in extensive outreach with other cities, state legislators, taxpayers and the business community to understand the interests of these stakeholders in relation to development of the Portal; and

WHEREAS, the creation of an intergovernmental entity, in the form of a governmental nonprofit corporation whose members are Principals to oversee the operation of the Portal will enable each Principal to participate in management of the Portal, provide economies of scale to participating cities, and ensure continued control by each Principal of its tax and licensing policy and local tax collections; and

WHEREAS, the collection of local taxes is an exclusively governmental activity of each of the cities party to this Agreement; and

WHEREAS, the creation of an intergovernmental entity as described in this Agreement will enable the Principals to carry out this exclusively governmental activity as a joint instrumentality; and

WHEREAS, it is anticipated that additional cities will elect to use the Portal over time, and that some may wish to do so as subscribers of the Portal's services rather than as principals; and

WHEREAS, The City of Seattle has provided start-up funding for the development of the Portal and has conducted a competitive procurement process in which staff from each of the Principals participated with Seattle staff in selecting a preferred vendor to provide portal development, hosting and maintenance services; and

WHEREAS, The City of Seattle has entered into a contract with the preferred vendor, and the vendor has begun work to develop the Portal with continued input from staff from each of the Principals;

NOW THEREFORE, in consideration of the promises and agreements contained in this Agreement and subject to the terms and conditions set forth, it is mutually understood and agreed by the Parties as follows:

SECTION 1. CREATION OF WASHINGTON MULTI-CITY BUSINESS LICENSE AND TAX PORTAL AGENCY.

The Washington Multi-City Business License and Tax Portal Agency, ("PORTAL AGENCY") is hereby created as authorized by the Interlocal Cooperation Act (Ch. 39.34 RCW), and shall be a municipal instrumentality of the Principals, jointly organized by the Principals as a nonprofit corporation under Chapter 24.06 RCW as expressly authorized by RCW 39.34.030(3)(b). The Principals each assign to PORTAL AGENCY the responsibility for overseeing the development, operation and maintenance of an internet web application gateway to administer city business licensing and tax collection functions as exclusively governmental activities, all as described herein.

SECTION 2. TERM OF AGREEMENT.

This Agreement shall have an initial term of approximately five years, ending on December 31, 2019, (the "Initial Term"), and shall thereafter be perpetual, subject to the termination provisions in Section 19 of this Agreement. During the Initial Term no Principal may withdraw from the Agreement, provided that a Principal may convert or be converted to Subscriber status as provided in Sections 8.a, 13.d and 13.k, and may upon action of the Executive Board be terminated from participation in the Agreement as provided in Section 13.k.

SECTION 3. DEFINITIONS.

a. Agreement. The "Agreement" is this interlocal agreement, as it may hereafter be amended or modified, together with all exhibits and appendices hereto, as they may hereafter be amended or modified.

b. Articles of Incorporation. The "Articles of Incorporation" or "Articles" are terms defining aspects of the PORTAL AGENCY corporate formation under 39.34.030(3)(b) and consistent with RCW 24.06.025, as they may hereafter be amended by the Executive Board.

c. Board Member. A "Board Member" or "Executive Board Member" is the individual representing a Principal on the Executive Board, whether the Chief Financial Officer of such Principal or his/her designated alternate.

d. Business and Occupation Taxes. "Business and Occupation Taxes" are Gross Receipt Taxes imposed by a Participating City as an exclusively governmental activity authorized by state law and as defined in RCW 35.102.030.

e. Business Licenses. "Business Licenses" are licenses required to be obtained by businesses in order to operate within a Participating City, consistent with state law.

f. Bylaws. "Bylaws" as adopted and amended from time to time by the Executive Board shall govern the operations of the PORTAL AGENCY Executive Board, Operations Committee, and the officers thereof.

g. Capital Cost Recovery Charge. The "Capital Cost Recovery Charge" is an annual fee charged to all Participating Cities other than the City of Seattle, for the purposes of reimbursing Seattle for a portion of the funding it provided to pay for start-up of the PORTAL AGENCY, as further described in Section 13.j.

h. Capped Costs. "Capped Costs" means all items in the PORTAL AGENCY budget *excluding*:

i. Labor Costs unrelated to increases in full or partial staff positions;
ii. Costs payable pursuant to the Portal Services Contract with the Vendor;
iii. State Auditor's Office Audit costs;
iv. Accounting services;
v. Insurance;
vi. Bank fees;
vii. Any unanticipated expenses outside the normal course of business, for example, costs of litigation or damages, uninsured losses, tax or other liabilities resulting from a change in law, and events of force majeure (e.g. fire, explosion, accident, volcanic eruption, flood, epidemic, civil disturbance).

i. CPI-U Limit. "CPI-U Limit" means the percentage increase (or decrease) equal to the percentage increase (or decrease) year to year in the Consumer Price Index – Urban for the Seattle/ Tacoma/Bremerton metropolitan area, April –April, calculated by the Federal Bureau of Labor Statistics, or its successor index.

j. Executive Board. The "Executive Board" is the body described in Section 7 and shall be the governing body of the PORTAL AGENCY.

k. Gross Receipts Taxes. "Gross Receipts Taxes" are taxes imposed by Participating Cities which are based on the gross receipts of certain businesses, specifically to include Business and Occupation Taxes as defined by RCW 35.102.030 as well as other taxes imposed by Participating Cities on utilities or businesses that are collected on basis of such gross receipts in accordance with applicable law. For purposes of this Agreement, Gross Receipts Taxes also includes square footage taxes imposed by a Participating City for the act or privilege of doing business in that city and calculated based on the amount of space occupied and used for those business activities within that city.

l. Initial Term. The "Initial Term" is the period from the effective date of this Agreement through December 31, 2019.

m. Labor Costs. "Labor Costs" include salary, benefits and other compensation provided to Portal Agency employees (if any) and/or loaned staff.

n. Licensees. "Licensees" are businesses or individuals that apply for a Business License from a Participating City or Cities using the Portal.

o. Manager. The "Manager" is the chief operating officer for PORTAL AGENCY appointed by and serving at the pleasure of the Executive Board.

p. New Participant Capped Cost Increment. The "New Participant Capped Cost Increment" is an amount calculated each budget period to identify the maximum amount by which Capped Costs may increase in the Executive Board approved draft or final budget for such period without unanimous approval of the Executive Board Members representing all Original Principals, as further described in Section 13.b.iv.1 and Exhibit D.

q. New Participant Labor Cost Increment. The "New Participant Labor Cost Increment" is an amount calculated each budget period to identify the maximum amount by which Labor Costs may increase to provide for additional full or partial staff positions in the Executive Board approved draft or final budget for such period without requiring unanimous approval of the Executive Board Members representing all Original Principals, as further described in Section 13.b.iv.2 and Exhibit D.

r. Operations Committee. The "Operations Committee" or "Tax and Finance Operations Committee" is the committee described in Section 9.

s. Original Principals. The Original Principals are those four cities initially signing this Agreement: the cities of Bellevue, Everett, Seattle and Tacoma.

t. Participating Cities. All Principals, and all Subscribers, as they may be so constituted from time to time, are collectively referred to as the "Participating Cities" or "Participants," and individually referred to as a "Participating City" or "Participant."

u. Population. "Population" is the residential population of a City, according to the most recent annual report issued by the State Office of Financial Management each year determining the population of each city for purposes of taxation and allocation of certain state shared revenues in the following calendar year.

v. Portal. The "Portal" is an internet web application gateway owned, operated and maintained by the Vendor under contract with the PORTAL AGENCY that affords Taxpayers and businesses a single access point through which they may apply for business licenses from, and pay taxes and fees to, Participating Cities, and receive information related to these functions.

w. PORTAL AGENCY. "PORTAL AGENCY" means the Washington Multi-City Business License and Tax Portal Agency.

x. Portal Operations Policy. The "Portal Operations Policy" is a separate document adopted by Supermajority Vote of the Executive Board, as it may be amended from time to time, which describes how data will be shared between the Participating Cities and the PORTAL AGENCY, and sets forth operating procedures and rules for the Portal.

y. Portal Services Contract. The 'Portal Services Contract" is that certain contract dated as of September 6, 2013 between The City of Seattle and ~~eGov~~Avenu Systems, a Louisiana corporation, to develop software for, and host the Portal operations. The Portal Services Contract is to be assigned to the PORTAL AGENCY by The City of Seattle pursuant to Section 12 of this Agreement.

z. Principal. A "Principal" is a general purpose municipal corporation formed as a city under the laws of the state of Washington which imposes a Business and Occupations Tax and which has accepted the terms of and is a party to this Agreement and has paid its share of initial costs as may be required by the Executive Board as a condition to becoming a Principal. Principals shall receive services offered by the PORTAL AGENCY according to such terms and conditions as may be established by the Executive Board.

aa. Representative. The term "Representative" refers to the individual representing a Principal or a Subscriber on the Operations Committee, or his/her designated alternate.

bb. Simple Majority Vote. A "Simple Majority Vote" of the Executive Board means a majority (more than 50%) of the votes of the Board Members present constituting a quorum, with each Board Member that is present and voting having one vote.

cc. Subscriber. A "Subscriber" is a general purpose municipal corporation, formed as a city under the laws of Washington which has agreed to pay the PORTAL AGENCY for services according to such terms and conditions as may be established by the Executive Board and evidenced by separate contract between the PORTAL AGENCY and such entity. A Principal may convert or be converted to Subscriber status as provided in Sections 8, 13.d and 13.k and a Subscriber may convert to a Principal as described in Section 8.

dd. Supermajority Vote. A "Supermajority Vote" means Executive Board approval of an item accomplished by securing affirmative votes of not less than sixty-six percent (66%) of all voting Board Members of the Executive Board in number, and not less than sixty-six percent (66%) in number of the Original Principals.

ee. Taxpayers. "Taxpayers" are businesses subject to local city taxes imposed by a Principal or Subscriber, payment of which is or can be administered by the Portal.

ff. Transaction. A "Transaction" is a payment or filing for a Business License, or a payment or filing of an online tax form (where multiple taxes filed on the same online tax form are counted as a single Transaction), made on the Portal by a business to a Participating City; *provided, however,* that where historical actual Transactions counts are to be used (rather than payments and transactions made *on the Portal*), then Transactions includes the total actual Business License filings and Gross Receipts Tax filings (where multiple taxes filed on the same tax form are counted as a single Transaction) for the Participating City over the applicable period. The Executive Board may refine this definition from time to time by amending the Portal Operations Policy in order to accommodate expansion of services offered by the Portal or to address other issues.

gg. User Fees. "User Fees" are fees and charges imposed on businesses, Licensees or Taxpayers per Executive Board approval as part of PORTAL AGENCY's budget approval process.

hh. Vendor. The Vendor is ~~eGov~~Avenu Systems, a Louisiana corporation, which through the Portal Services Contract is providing services to develop, establish, host, own and maintain the Portal, associated online data storage and services. The Vendor has ownership of the Portal. The term Vendor shall also include any successor in interest to ~~eGov~~Avenu Systems or any successor firm(s) or agency(s) with which the PORTAL AGENCY may contract to provide Portal development, hosting, maintenance, and associated online data storage and services.

SECTION 4. GUIDING PRINCIPLES AND GOALS.

a. Guiding Principles of PORTAL AGENCY. The Principals intend that the PORTAL AGENCY actions be guided by the following guiding principles:

i. Local Control – The PORTAL AGENCY will seek to respect and preserve each Participating Cities' authority to set local tax policies.

ii. Integrity – The PORTAL AGENCY will be honest, truthful and straightforward.

iii. Accountability – The PORTAL AGENCY will be responsible for its actions and decisions, a good steward of public funds and transparent in its operations.

iv. Flexibility / Adaptability – The PORTAL AGENCY will strive to nimbly respond to a changing business, technology and policy environment.

v. Security – The PORTAL AGENCY will at all times seek to safeguard Taxpayer, Licensee and Participating City data.

vi. Accessibility – The PORTAL AGENCY will seek to be accessible and responsive to Taxpayers, Licensees and Participating Cities.

vii. Affordability – The PORTAL AGENCY will seek to be affordable to both Participating Cities and businesses and taxpayers using the Portal. Also, fees

and charges will be structured so that the addition of new Cities using the Portal does not impose additional costs on prior Participating Cities.

b. Goals of the PORTAL AGENCY. The Principals acknowledge and support the following goals which they seek to accomplish by this Agreement and creation of the PORTAL AGENCY:

i. Taxpayers and Licensees utilizing the Portal will have a seamless, transparent, user-friendly and efficient experience.

ii. It will be easy and timely for Taxpayers and Licensees to access knowledgeable staff at each Participating City to respond to tax or licensing questions.

iii. The Portal will have error-free data collection, transmittal and tax payment allocation as between Participating Cities.

iv. There will be local control and oversight of tax collections and tax policy.

v. Participating Cities will be accountable for the accuracy and timeliness of information they provide to the PORTAL AGENCY and for their customer service response.

vi. Decision-making will by jointly exercised by the Principals through the Executive Board.

vii. The PORTAL AGENCY will seek to balance the interests of information technology, treasury, finance and tax staff within Participating Cities in the development of the Portal's capabilities and operating rules.

viii. The PORTAL AGENCY will comply with all legal requirements, including but not limited to public record-keeping, public meetings, public records, security, and audit requirements.

ix. The PORTAL AGENCY will be able to accommodate additional city partners as Principals or Subscribers over time and be able to process additional types of local taxes and licenses over time.

x. The PORTAL AGENCY will support the ability to maximize use of the Portal by Taxpayers and Licensees so that Participating Cities do not need to replicate the Portal's services.

xi. The PORTAL AGENCY will maximize compatibility with Participating City's systems of record for data storage and processing.

xii. The PORTAL AGENCY will coordinate with the state Department of Revenue.

xiii. The PORTAL AGENCY will be a cost-effective solution for Participating Cities.

SECTION 5. PORTAL AGENCY SERVICES.

a. Generally. The PORTAL AGENCY has the responsibility and authority for overseeing the Vendor's contractual responsibilities to develop, own, operate, maintain and manage the Portal and for managing the operations of the PORTAL AGENCY. It is expressly contemplated that this scope of services includes:

i. The implementation, operation and maintenance of replacement or upgrades of the Portal as necessary or appropriate.

ii. The development and adoption of rules for access, use and maintenance of the Portal by City Participants, Taxpayers and Licensees.

iii. Expansion of the scope of services offered through the Portal if approved per Subsection 5.c below.

iv. Other responsibilities reasonably necessary for the development, operation and maintenance of the Portal.

v. Other related or ancillary services.

b. Limitation on Authority. The PORTAL AGENCY shall have no authority to set tax rates or tax classifications for Participating Cities, to set local tax policy, tax rules, deductions or exemptions; or take enforcement action on behalf of any Participating City. The PORTAL AGENCY is created by the Principals to manage the Participating Cities' joint participation in the facilitation of an exclusively governmental activity, specifically, the collection of certain local taxes.

c. Expansion of Scope of Services. The Portal will be initially established with the capability to handle payment of Gross Receipts Taxes and filing of applications for Business Licenses. PORTAL AGENCY may provide additional capability to pay additional types of city taxes or application for additional types of city licenses through the Portal only upon approval of a Supermajority Vote of the Executive Board; *provided, however,* that the cost of service expansions will be allocated only to those Participating Cities electing to participate in such services.

d. Requirement of Participating Cities to Utilize Services of Portal**.**

i. Gross Receipts Tax Collection Services: Participating Cities shall be required to offer their Taxpayers the option of paying Gross Receipts Taxes through the Portal, if and to the extent such taxes are imposed by a Participating City.

ii. Other Services: Except as required by Subsection 5.d.i above, no Participating City shall be required to utilize any other service of the Portal without the prior written approval of such City.

iii. Provision of Alternate Collection Options by Participating Cities. Nothing in this Agreement shall be interpreted to preclude a Participating City from

offering its Taxpayers or businesses additional means (other than through the Portal) for acquiring Business Licenses or paying any local taxes, including but not limited to payment of Gross Receipts Taxes.

iv. Operating Policies and Rules for Use of Portal. In order to protect sensitive Taxpayer data and assure the relationship between the Portal and Participating Cities remains fully functional and secure, the Executive Board shall adopt a Portal Operations Policy. It is understood and agreed that the access and use of the Portal by any Principal or Subscriber is conditioned on that party consenting in writing to comply with the Portal Operations Policy. Such consent shall be signified by signature of the chief executive officer of each Participating City, or his/her designee, and shall not require further legislative action of the Participating City. The Portal Operations Policy will be regularly reviewed and updated by the Executive Board as necessary or appropriate.

e. Additional Activities of the PORTAL AGENCY. At the discretion of the Executive Board, the PORTAL AGENCY may, in addition to the services described in Section 5.a above:

i. Participate in forums for Participating Cities to discuss tax policy issues (including but not limited to the Association of Washington Cities Tax Policy Advisory Group or its successor in interest);

ii. Provide education to Taxpayers and Businesses regarding the Portal and the PORTAL AGENCY, and work to increase transparency about Participating City tax policies and activities;

iii. Provide a forum for businesses and others to provide feedback and suggestions on the use and functionality of the Portal and the taxes and licenses administered through the Portal; and

iv. Provide a forum for discussion, coordination and execution of coordinated enforcement activities, provided that the PORTAL AGENCY itself is not authorized to take any tax collection or license fee enforcement actions on behalf of a Participating City. The PORTAL AGENCY shall not use or authorize the use of the Portal or such forum for the purpose of assisting a campaign for election of any person to any office or for the promotion of or opposition to any ballot proposition.

v. The PORTAL AGENCY shall coordinate with the Washington State Department of Revenue with regard to the Portal's operations and functionality to minimize the need for Taxpayers and Licensees to enter data on the Portal and any separate state tax payment and licensing systems.

SECTION 6. PORTAL AGENCY POWERS.

Through its Executive Board**,** the PORTAL AGENCY shall have all powers allowed by law for interlocal agencies created under RCW 39.34.030 and Chapter 24.06 RCW, as authorized, amended, or removed by the Executive Board, as provided for in this Agreement and including but not limited to the following:

a. Recommend action to the legislative bodies of the Participating Cities;

b. Review and approve budget expenditures for the PORTAL AGENCY;

c. Establish policies for expenditures of budget items for the PORTAL AGENCY;

d. Review and adopt a personnel policy for the PORTAL AGENCY (if applicable);

e. Review and approve operating, Portal use, and financial policies for the PORTAL AGENCY;

f. Establish a fund or special fund or funds as authorized by RCW 39.34.030 for the operation of the PORTAL AGENCY;

g. Conduct regular and special meetings as may be designated by the Executive Board consistent with the state Open Public Meetings Act (Ch. 42.30 RCW) as now or hereafter amended;

h. Maintain and manage records in accordance with the state Public Records Act (Ch. 42.56 RCW) as now or hereafter amended, and other applicable state and federal laws and regulations;

i. Determine what services shall be offered and under what terms they shall be offered, consistent with Section 5.

j. Retain and terminate a Manager;

k. Create committees to review and make recommendations and carry out such functions and responsibilities as the Board may expressly provide;

l. Approve strategic plans;

m. Approve the addition of new Principals and new Subscribers and the terms of their participating in PORTAL AGENCY and receipt of PORTAL AGENCY services;

n. Enter into agreements with third parties for goods and services necessary to fully implement the purposes of this Agreement;

o. Establish fees and charges for services provided to Participating Cities or other parties, including but not limited to Taxpayers and Licensees using the services of the Portal;

p. Direct and supervise the activities of any committee established and/or any advisory boards, and the Manager;

q. Accept grants of funds from any federal, state, local or private agencies and receive and distribute such funds;

r. Receive all funds allocated to PORTAL AGENCY by Participating Cities;

s. Purchase, take, receive, lease, take by gift, or otherwise acquire, own, hold, improve, use and otherwise deal in and with real or personal property, or any interest therein, in the name of PORTAL AGENCY;

t. Sell, convey, lease, exchange, transfer, and otherwise dispose of all of its property and assets;

u. Sue and be sued, complain and defend, in all courts of competent jurisdiction in PORTAL AGENCY's name;

v. Make and alter bylaws for the administration and regulation of its affairs; and

w. Any and all other lawful acts necessary to further PORTAL AGENCY's goals and purposes.

x. Notwithstanding the foregoing, the PORTAL AGENCY shall not have the authority to issue debt in its own name.

The Portal Agency, as a joint instrumentality of its municipal corporation members under Chapter 39.34 RCW, shall have no powers or authority that are not held by Washington cities.

SECTION 7. EXECUTIVE BOARD: COMPOSITION AND OPERATION.

a. Composition. The Executive Board shall be composed of one (1) Board Member from each Principal, plus at least one (1) non-voting Board Member representing PORTAL AGENCY Subscribers. Such representatives are referred to as a Board Member or Board Members of the Executive Board.

b. Powers. The Executive Board shall have final decision-making authority upon all policy issues and shall exercise the powers described in Section 6**.** The Executive Board may delegate responsibility for execution of Executive Board policies and directives and for day-to-day operational decision-making to the Manager, including the hiring and supervision of additional staff positions authorized by the Executive Board, subject to the terms of Section 11.

c. Limitation on Total Number of Voting Board Members on Executive Board; Allocation of Executive Board Positions Among Multiple Principals. Notwithstanding the terms of Subsection 7.a, at no time shall the number of Executive Board Members exceed fifteen (15) voting members, and for so long as it remains a Principal, no Original Principal shall be required to share representation of its Board seat with another Principal. If the addition of a new Principal would cause the number of Executive Board voting Board Members to exceed fifteen (15), then the Principals with the smallest Population shall share a single Board Member position in order to reduce the number of Executive Board voting Board Members to fifteen (15); *provided that*, if over five (5) Principals would be represented by a single Board Member, then an additional

Board seat shall be converted for shared representation, to be shared by the Principals with the smallest Population. In the event that the number of Principals sharing representation is not evenly divisible by the number of shared seats, then the Principals with the larger Population shall be given the benefit of the allocation (e.g., if 7 Principals are to share 2 seats, then the 3 Principals with the largest Population (within the group sharing representation) shall share one (1) seat, and the four (4) Principals with the smallest populations shall share the second seat). If the number of Principals exceeds 59, then the same process as described above shall be repeated, that is, moving to a maximum of six (6) Principals sharing a seat, and so on (seven (7) Principals sharing a seat, etc.) as necessary to accommodate additional Principals.

d. Method of Determining Selection of Subscriber Representative(s) or Shared Voting Board Member(s). Subscribers shall initially share one (1) non-voting seat on the Executive Board. The Executive Board may by Supermajority Vote increase the number of non-voting seats for Subscribers and may define how such additional seats are allocated among Subscribers. Unless otherwise described in the Bylaws, Subscribers sharing representation of the non-voting Board Member shall determine the means by which to select their Executive Board representative and shall inform the Board of their choice at the time of the biennial Executive Board Officer elections (or at such other times as may be required in the event of a vacancy). Similarly, those Principals sharing representation on a single Executive Board seat shall determine the means by which to select the position, and shall make the determination at the same time as the biennial Executive Board Officer elections (or at such other times as may be required in the event of a vacancy).

i. Unless otherwise described in the Bylaws, in the event that Subscribers or Principals are unable to agree on a shared representative or Board Member on a timely basis, the remaining Executive Board Members may make the selection for them by a vote of the Executive Board.

ii. Individuals representing multiple Subscribers or Principals are expected to confer with the Cities they represent.

e. Qualifications to Serve on Executive Board. To serve on the Executive Board, as either a voting or non-voting Board Member, a person must be the appointing city's Chief Financial Officer (e.g., finance director or city treasurer, or equivalent), or their deputy or equivalent. An individual representing multiple cities on a single Executive Board seat or serving as the non-voting Subscriber representative shall similarly hold such a position within one of the Subscriber cities sharing such representation.

f. No Compensation for Serving on Executive Board. All Executive Board Members and their alternates shall serve without compensation from the PORTAL AGENCY. However, the PORTAL AGENCY may pay for or reimburse Executive Board Members and alternates for out-of-pocket costs related to service on the Executive Board.

g. Term of Office; Vacancies**.** Executive Board Members shall serve on the Executive Board for so long as they hold a position that qualifies them for the seat unless the city they represent elects to appoint another individual. Executive Board Members representing multiple Cities (either as a Principal or Subscriber) shall serve until the next Board Officer elections. Any vacancies shall be promptly filled by the appointing Principal, group of Principals, Subscribers, or the Executive Board (per Section 7.d.i), as appropriate.

h. Alternates. Each Executive Board Member shall have a single alternate designated in writing. Alternates must meet the same qualification as the designated Board Member or have similar financial expertise and be in a management position within their city.

i. Quorum. A simple majority of the Board Members (or their alternates) in number (excluding any Board Member which per Section 17 has given notice of withdrawal or which has been terminated by vote of the Executive Board) shall constitute a quorum of the Executive Board for purposes of taking action.

j. Voting. The Executive Board shall strive to operate by consensus. All Executive Board decision on items not listed in Section 7.k shall require a Simple Majority Vote for approval. A Board Member may not split his or her vote on an issue. No voting by proxies or mail-in ballots will be allowed. Voting by a designated Alternate is not considered a vote by proxy. A Board Member representing a Principal that has given notice of withdrawal or which has been terminated by vote of the Executive Board shall be authorized to cast votes at the Executive Board only on budget items to be implemented prior to the withdrawal or termination date.

k. Items Requiring a Supermajority Vote for Approval:

i. Approval or amendment of the budget or draft budget. (Per Section 13.b.iv, approval of the draft and final budget or amendments thereto also requires unanimous approval of the Original Principals in certain instances).

ii. Approval or amendment of user fees and charges.

iii. Approval of the Portal Operations Policy or amendments thereto.

iv. Adoption or amendment of the Bylaws or amendment of the Articles of Incorporation.

v. A decision to acquire assets, equipment, real or personal property, or bind the PORTAL AGENCY to pay total or cumulative any contract amounts over $50,000, *provided that,* this threshold amount will be indexed on the fifth anniversary of the formation of the PORTAL AGENCY and every five (5) years thereafter by the CPI-U Seattle-Tacoma-Bremerton.

vi. Admission of a new Principal.

vii. Admission of a new Subscriber.

viii. The decision to create an additional non-voting seat for Subscribers on the Executive Board.

ix. Addition of any staff positions, or partial staff positions, to support PORTAL AGENCY operations. (Per Section 13.b.iv, approval of funding for increases in the number of staff positions also requires unanimous approval of the Original Principals in certain instances).

x. Appointing or removing the Manager.

xi. Merger, consolidation, sale of all or substantially all assets of the PORTAL AGENCY (See Section 16).

xii. Amendment of the Agreement (except for those amendments requiring approval of all legislative bodies of the Principals per Section 18).

xiii. Termination or dissolution of the PORTAL AGENCY (See Section 19).

xiv. Any other action actions requiring a sixty-six percent (66%) Supermajority vote under Chapter 24.06 RCW.

l. Officers. The Executive Board shall have four officers, a Chair, Vice-Chair, Secretary and Treasurer. It will be the function of the Chair to preside at the meetings of the Executive Board. The Vice-Chair shall assume this role in absence of the Chair. At the first meeting of the Executive Board following the effective date of this Agreement, the officers shall be elected, and shall serve in this capacity through April 1, 2016, whereupon a new Chair and Vice-Chair shall be elected by the Executive Board. Biennially thereafter, the Executive Board shall elect a new Chair and Vice-Chair for two (2) year terms commencing each April 1. In the event of a vacancy in the Chair position, the Vice-Chair shall assume the Chair for the balance of the term of the departed Chair. In the event of a vacancy in the Vice-Chair position, the Executive Board shall elect a new Vice-Chair to serve the balance of the term of the departed Vice-Chair. An officer elected to fill the unexpired term of his or her predecessor shall not be precluded from serving one or more full annual terms of office following the end of such unexpired term. Any officer appointed by the Executive Board may be removed by vote of the Executive Board, with or without cause, in which event the Executive Board shall promptly elect a new officer who shall serve until the next regular officers' board term begins. The Executive Board may appoint persons other than Board Members of the Executive Board to serve as Secretary and Treasurer of the PORTAL AGENCY. The duties of all officers shall be further described in the PORTAL AGENCY Bylaws.

m. Staffing. The Manager shall assign agency staff to support the Executive Board as he or she deems appropriate.

n. Meetings. The Executive Board shall meet as often as it deems necessary and not less than once a year, at a time and place designated by the Chair of the Executive Board or by a majority of its Board Members. Not less than fourteen (14) days advance notice of regular

meetings shall be given. Special meetings may be called by the Chair or any two (2) Board Members upon giving all other Board Members not less than ten (10) days prior notice. In an emergency, the Executive Board may dispense with written notice requirements for special meetings, but must, in good faith, implement best efforts to provide fair and reasonable notice to all Executive Board Members. Board Members (or alternates) may participate in meetings by telephone conference or equivalent means of voice communication. At all times, the Executive Board shall comply with Ch. 42.30 RCW (Open Public Meetings Act).

o. Articles of Incorporation and Bylaws. Unless otherwise provided in the Articles and Bylaws or by vote of the Executive Board, upon the request of any Board Member of the Executive Board, Robert's Revised Rules of Order shall govern any proceeding of the Executive Board.

p. Consultation with Operations Committee. It is the intent of this Agreement to seek the active participation and advice of Participating Cities in the determination of PORTAL AGENCY policies and management. To the extent practicable, all items to come before the Executive Board shall have been previously subject to the review, comment and recommendation of the Operations Committee and the Executive Board shall consider input from the Operations Committee in its deliberations.

q. Consultation with Businesses, Taxpayers and Participating Cities. Not less than once each year the Executive Board shall seek input from Taxpayers and Participating Cities for the purpose of securing feedback and information on the efficiency and effectiveness of the Portal and PORTAL AGENCY programs.

SECTION 8. CONVERSION OF STATUS OF PARTICIPATING CITIES; ADDITION OF NEW PRINCIPALS OR SUBSCRIBERS.

a. Loss of Principal Status. As described in Sections 13.d and 13.k hereof, a Principal shall be converted to Subscriber for failure to approve its share of the budget or for nonpayment or delinquency in payment of charges and fees. On the date of such conversion, said former Principal shall:

i. lose its representation on the Executive Board;
ii. lose its right to receive a share of the PORTAL AGENCY assets upon dissolution of the PORTAL AGENCY;
iii. become subject to payment of charges and fees in accordance with the then applicable payment formula for Subscribers; and
iv. be bound by the terms of the then current Subscriber service contract.

The conversion of a Principal to Subscriber shall not discharge or relieve any Principal of its obligations to the PORTAL AGENCY or any other Participating City.

b. Election to Convert to Subscriber. A Principal may elect to convert to Subscriber status effective the first day of the next budget period by giving notice of its intent to the Governing Board not less than eight (8) months in advance of such effective date; *provided that*, a Principal may not exercise such election to take effect within the Initial Term. Such conversion shall be effective as proposed without further action of the Executive Board, barring any basis for terminating the Principal and action thereon by the Executive Board.

c. New Principals. A city or town otherwise meeting the qualifications of a Principal in Section 3.z hereof may be admitted to the PORTAL AGENCY as a Principal upon Supermajority Vote of the Executive Board as required under Section 7.k and its approval and execution of a document confirm. Similarly, a Subscriber may apply to the Executive Board to be converted to Principal status. As a condition of becoming a Principal, whether by conversion or new admission, the Executive Board may require payment or other contributions or actions by the new Principal as the Executive Board may deem appropriate consistent with the Bylaws and Portal Operations Policy, and may set such start date for service as it deems appropriate, it being the intention that the addition of new Principals shall not cause then-existing Principals to incur additional costs.

d. New Subscribers. The determination of whether to accept Subscribers shall be made by the Executive Board in a manner similar, and subject to such terms and conditions, as that for accepting new Principals, it being the intention that the addition of new Subscribers shall not cause then-existing Principals or Subscribers to incur additional costs.

SECTION 9. TAX AND FINANCE OPERATIONS COMMITTEE.

a. Role and Responsibilities. A Tax and Finance Operations Committee ("Operations Committee") shall be established to provide advice and recommendations to the Executive Board. The Executive Board may determine to direct the Operations Committee to perform specific responsibilities within Board-defined parameters. The Operations Committee shall endeavor to promote interagency collaboration, cooperation and information sharing between PORTAL AGENCY Principals and Subscribers. The Operations Committee shall:

i. Assist in the review and development of Portal Operations Policy and amendments thereto, Portal development options, proposed new service options, and such other matters as the Executive Board may direct;

ii. Make reports and recommendations to the Executive Board from time to time on matters the Operations Committee deems appropriate;

iii. Assist in the review and development of proposed PORTAL AGENCY budgets;

iv. Provide written recommendations with respect to the proposed budget to the Executive Board at the time the proposed budget is submitted to the Executive Board;

v. Provide advice, information and recommendations to the PORTAL AGENCY Manager and staff;

vi. Assist in communications to City Councils, legislators, business community on PORTAL AGENCY issues;

vii. Reach out to technology staff within their respective Cities for input and ideas, and to keep them apprised of PORTAL AGENCY issues;

viii. Brief their respective Executive Board Members in advance of Executive Board meetings.

b. Membership. Membership of the Operations Committee shall include one (1) Representative from each Principal, appointed by that Principal, plus at least one (1) representative, appointed by the Executive Board, to represent Subscribers. Each Principal shall also appoint in writing a designated alternate to serve on the Operations Committee in case of absence of the primary Representative**.**

c. Qualification to serve on Operations Committee. Representatives and their alternates shall be staff from the Principal they represent, with expertise in city tax policy and administration and/or city financial policy and administration. Persons serving on the Operations Committee are referred to as Representatives (or alternates) and shall serve without compensation from the PORTAL AGENCY.

d. Officers, Voting, Meeting Rules. The Operations Committee shall select a Chair and Vice-Chair from among the membership of the Operations Committee. Each Representative on the Committee shall have one vote. The meeting rules for the Operations Committee shall be further defined in the PORTAL AGENCY Bylaws.

e. Staffing. The Operations Committee shall be staffed by the Manager and such additional agency staffing as the Manager may deem appropriate.

SECTION 10. PORTAL AGENCY STAFFING.

a. The PORTAL AGENCY shall be staffed in such manner as the Executive Board determines, including but not limited to the use of loaned employees from Principals, consultants or other service providers, purchase of services from Principals or others, or hiring staff, or any combination of the foregoing.

b. As described in Section 13.b.iv.2 and Exhibit D, any increase in Labor Costs in excess of the New Participant Labor Cost Increment requires approval of a Supermajority Vote of the Executive Board as well as the approval of all Board Members representing all Original Principals.

SECTION 11. PORTAL AGENCY MANAGER.

a. Portal Agency Manager Appointment, Responsibilities and Authority. The Executive Board shall be responsible for the appointment and termination of a Manager of the PORTAL AGENCY, and shall request input from the Operations Committee, or any other standing committees created by the Executive Board, regarding any proposed appointment. The Manager shall:

i. Be responsible to the Executive Board and shall advise it from time to time on a proposed budget and other appropriate matters in order to fully implement the purposes of this Agreement;

ii. Administer the PORTAL AGENCY in its day-to-day operations consistent with the policies adopted by the Executive Board;

iii. Appoint persons to fill other staff positions, subject to confirmation by the Executive Board as the Board may require;

iv. Submit quarterly budget and operation performance reports to the Executive Board in a form acceptable to the Executive Board;

v. Undertake outreach to Taxpayers, Licensees and businesses, as well as to Participating Cities on the effectiveness of the PORTAL AGENCY operations and programs.

vi. Manage and oversee performance of the Vendor and other vendors or contractors providing services to the PORTAL AGENCY.

vii. Consult in advance with the Operations Committee on issues to come before the Executive Board, including but not limited to working with the Operations Committee in the development of the PORTAL AGENCY's budget and policies.

b. Qualifications, Retention and Termination. The Manager shall have experience in technical, financial and administrative fields and his or her appointment shall be on the basis of merit only. The Manager is an "at will" position and may be terminated from his or her position as Manager upon the Supermajority Vote of the Executive Board, without cause.

c. Legal Counsel, Accountants and Auditors. Only the Executive Board shall be authorized to hire or retain legal counsel and independent accountants and auditors. Other consultants may be designated in such manner as the Executive Board may determine subject to Sections 6 and 7.

d. Contracts and Support Services. Subject to the terms of the Bylaws, the Executive Board or the Manager with advice of the Operations Committee shall as necessary contract with appropriate local governments or other third parties for the use of space for its operations, and for staff and auxiliary services including, but not limited to, records, payroll, accounting, purchasing and data processing. Notwithstanding the foregoing, only the Executive Board may approve changes to the Portal Vendor(s) or Portal Vendor Services Contract.

SECTION 12. ASSIGNMENT OF PORTAL SERVICES CONTRACT FROM SEATTLE TO PORTAL AGENCY.

Promptly following the execution of this Agreement and the filing of such forms with the Washington Secretary of State as are necessary to incorporate the PORTAL AGENCY as a nonprofit corporation, The City of Seattle agrees to assign the Portal Services Contract to the PORTAL AGENCY, together with all rights and responsibilities appurtenant thereto and the PORTAL AGENCY shall agree to accept such assignment, rights and responsibilities, it being the intent of the parties to this Agreement that the PORTAL AGENCY shall assume all responsibility for overseeing and funding the work of the Vendor pursuant to such Portal Services Contract as soon as practicable following formation of the PORTAL AGENCY.

SECTION 13. BUDGET; COST ALLOCATION; CAPITAL COST RECOVERY CHARGES; PAYMENT OF CHARGES; DELINQUENCIES; RESERVE FUNDS.

a. Budget Fiscal Year. The budget fiscal year shall be either the calendar year, or two calendar years as the Executive Board may determine. The "budget period" corresponds to the fiscal year or years so determined by the Board.

b. Budget Approval. The Manager shall develop the proposed operating budget in consultation with the Operations Committee. The Manager and Executive Board shall use their best efforts to meet the budget schedule set forth below, but failure to meet a specified budget deadline shall not constitute a breach of this Agreement.

i. The Manager shall present a proposed budget to the Executive Board by no later than **May 1** prior to the commencement of the budget period, together with the Operation Committee's recommendations with respect to the proposed budget.

ii. By no later than **June 15**, the Executive Board shall (1) review and revise the draft budget as it deems appropriate; (2) approve the draft budget (including proposed charges to Participating Cities and any user fees to

Taxpayers and Licensees) by Supermajority Vote; and (3) forward same to Principals. The approved draft budget, and all proposed fees and charges shall be forwarded to Subscribers no later than **July 1**.

iii. The final budget shall be adopted by vote of the Executive Board effective no later than **December 31** prior to commencement of the budget period, after receiving information as to:

1. which Subscribers will be continuing to contract with the PORTAL AGENCY; and

2. which Principals have or will approve their shares of the PORTAL AGENCY budget, based on action or information from such Principals received by the PORTAL AGENCY no later than **December 1**.

iv. Vote Required to Approve Budget. Per Section 7.k.i, a Supermajority Vote of the Executive Board is required to approve the draft and final budget, *provided* that unanimous approval of the Executive Board Members representing all Original Principals shall also be required to approve any budget or budget amendment that includes:

1. An increase in Capped Costs greater than the maximum amount allowed per calculation of the New Participant Capped Cost Increment, as further described in Exhibit D.

2. An increase in Labor Costs to increase the number of full or partial staff positions greater than the maximum amount allowed per calculation of the New Participant Labor Cost Increment, as further described in Exhibit D.

v. 2014 Budget. Notwithstanding the foregoing, the PORTAL AGENCY budget for the year 2014 will be formally adopted by action of the Executive Board promptly following incorporation of the PORTAL AGENCY and need not be submitted for approval by the Original Principals. The proposed 2014 budget is set forth at Exhibit A. By approving this Agreement each Original Principal also approves their contribution to the 2014 budget in an amount not to exceed that shown in Exhibit A, promptly following the date the PORTAL AGENCY is incorporated.

c. Payment of Charges. The Board shall determine the timing of payments by Participating Cities, which shall be set forth in the Portal Operations Policy.

d. Failure of a Principal to Approve Budget Share. Failure of a Principal to approve its share of the budget before the commencement of the budget period shall result in the Principal being converted to Subscriber status effective as of the first day of the budget period for which the budget was not approved.

e. Notification of Final Adopted Budget. Promptly following final adoption of the budget by the Executive Board, the Manager shall provide notice to all Principals and Subscribers as to the terms of the final adopted budget, including their share of PORTAL AGENCY costs, charges and fees, and the payment schedule.

f. Budget Modifications. Modifications to the budget shall be approved by a Supermajority Vote of the Executive Board (and also unanimous consent of the Original Principals if required by Section 13.b.iv above) as necessary from time to time to account for changes in expenditures and revenues.

g. Cost Allocation and Cost Recovery Principles. The PORTAL AGENCY budget shall be generally allocated between all Participating Cities based on the number of Transactions processed for each City on the Portal. In years 2014 through 2018, the number of Transactions for the Original Principals shall be based on 2012 historical actual pre-Portal use Transaction Counts (set forth in Exhibit A) and the City Transaction Count for any other Participating City shall be based on the most recent historical data for that City prior to it joining the Portal. From and after 2019, the number of Transactions allocated to Original Principals shall be based on the most recent actual annual number of Transactions processed on the Portal for each such City (thus for 2019, the 2017 actual Transaction count will be used); for other Participating Cities, the allocation will be determined considering the actual number of Transactions (if the City had joined before 2019), historical tax and license information, and the experience of Original Principals as to how quickly businesses have adopted use of the Portal since its launch. The details of the cost allocation calculation shall be set forth in the Portal Operations Policy. Nothing in this Agreement shall be construed to prohibit the Executive Board from including factors in addition to the number of City Transactions in the cost allocation formulas as between Participating Cities, so long as the primary basis for allocation remains the City Transaction count.

h. User Fees. The PORTAL AGENCY shall impose such reasonable user fees as the Executive Board may determine on Taxpayers and Licensees utilizing the Portal to file tax returns or file business license applications in order to recoup costs of PORTAL AGENCY

operations, the Portal operation and maintenance, reserves and any other PORTAL AGENCY costs.

i. Estimated Six Year Operating Costs**.** Exhibit B sets forth a general estimate of the annual costs to establish and operate the PORTAL AGENCY between 2014 and 2020, assuming the Original Principals are the only Participating Cities, and includes estimated payment of Vendor's charges pursuant to the Portal Services Contract and other estimated operating costs. This Exhibit is an estimate and is not binding on any of the parties to this Agreement, nor is it binding on the PORTAL AGENCY.

j. Capital Cost Recovery Charge. In order to reimburse the City of Seattle for approximately one third of the costs Seattle paid to fund start-up of the Portal Agency, each Participating City other than the City of Seattle will be charged an annual Capital Cost Recovery Charge, in an amount described in Exhibit C. Such Charges shall be imposed each year from and after 2015 until such time as the total Capital Cost Recovery Charges paid reaches $1,400,000. The Capital Cost Recovery Charges will be paid by Participating Cities to the Portal Agency and the Portal Agency shall thereafter remit the total annual amount to Seattle. The Capital Cost Recovery Charge is not considered part of the Portal Agency budget for purposes of calculating Capped Costs or CPI-U limitations on the growth of such costs.

k. Payment and Delinquencies. Principals shall promptly pay fees and charges allocable to them. Interest on fees and charges allocable to any Principal not paid when due shall begin accruing interest immediately at the Federal Reserve Prime Rate as of the date the payment was originally due, plus 3% per year. The PORTAL AGENCY shall, within seven (7) days of the due date, send notice to any delinquent Principal and provide a 60-day cure period from the original due date of the payment. If such fees and interest penalties are not paid in full within 60 days of the original due date, then the Principal delinquent in payment of fees shall upon such 60th day be deemed immediately converted to the status of a Subscriber and subject to penalty as described in Section 8. In the event a Principal converted to Subscriber status by non-payment of fees shall not have paid in full all fees and interest owing by six (6) months after the original due date, then the Executive Board may terminate provision of the PORTAL AGENCY'S services to that former Principal. After one (1) year, the nonpaying former Principal shall be deemed to have withdrawn from this Agreement, but the termination of services shall not absolve the former Principal of its obligation to pay all fees and charges past due, together with interest.

l. Terms of Subscriber Contracts. Subscriber contracts shall include terms consistent with these delinquency provisions, that is, interest shall accrue on delinquent payments at the same rate as provided herein, and service may be terminated if fees and interest are not paid in full within six months.

m. Reserve Funds. The Executive Board may establish and fund reserve funds to support operations or capital investments for the PORTAL AGENCY, at levels the Executive Board determines to be appropriate; *provided* that general reserve funds may only be used to support general PORTAL AGENCY operations, maintenance and capital costs and may not be used in support of developing projects or services that will not be utilized by all Principals; and *provided further*, that no Principal shall be required to contribute to special reserves established exclusively in support of projects or services that the Principal has certified it does not intend to utilize or make available to its Taxpayers and Licensees.

n. Use of Funds. Consistent with any use imposed on particular funds by statute, ordinance, contract, this Interlocal Agreement or any bylaws adopted by PORTAL AGENCY, the PORTAL AGENCY may use any available funds for any purpose authorized by this Agreement in connection with an authorized project.

SECTION 14. RETAINED AUTHORITY AND RESPONSIBILITY OF PARTICIPATING AGENCIES.

Each Participating City shall retain the responsibility and authority for its operational departments and for such equipment and services as are required at its place of operation to connect to PORTAL AGENCY operations, including but not limited to each Participating City's computer and data systems managing processes that provide services the Portal delivers (the City's system of record). Each Participating City shall also retain the responsibility and authority for managing and maintaining the security and privacy of all data that the Participating City links to the Portal. Inter-connecting equipment and services will not be included in PORTAL AGENCY'S budget and operational program, except as the Executive Board may determine.

SECTION 15. OWNERSHIP OF PROPERTY.

a. Ownership of Property. Excepting the Portal which is owned by the Vendor, all property both real and personal, as well as intellectual property rights or licenses purchased or otherwise acquired pursuant to or in connection with this Agreement shall be owned or held in the name of the PORTAL AGENCY; provided, however, that the Executive Board may convey ownership of specific property, property or use rights.

b. Loaned Property. If any Participating City provides equipment or furnishings for PORTAL AGENCY'S use, title to the same shall rest with the respective local entity unless that equipment or furnishing is acquired by the PORTAL AGENCY.

c. Data. Each Participating City shall retain ownership of its own data and property that may be used in connection with Portal or PORTAL AGENCY operations.

SECTION 16. MERGER OR CONSOLIDATION, OR SALE OF ALL OR SUBSTANTIALLY ALL ASSETS.

Approval of the merger or consolidation of PORTAL AGENCY with another entity, or the sale of all or substantially all assets of PORTAL AGENCY, shall require a Supermajority Vote.

SECTION 17. WITHDRAWAL BY, OR TERMINATION OF, A PRINCIPAL.

a. Notice and Timing. Any Principal may withdraw its membership and terminate its participation in this Agreement by providing written notice to the Executive Board on or before December 31 in any year, and the Executive Board shall promptly inform all other Principals of such notice. That withdrawal shall become effective on the last day of the next calendar year. Notwithstanding the foregoing, no Principal may terminate its participation in this Agreement effective prior to the end of the Initial Term.

b. Obligations of departing Principal. A Principal who withdraws, is terminated, changes or is changed to Subscriber status ("departing Principal") shall hold the remaining Principals and Subscribers harmless against any resultant increased capital and/or operating costs allocated to them for the following two (2) budget years (plus the remainder of the current budget year, if applicable), with respect to any Executive Board approved project (excluding the initial launch of the Portal) in which the departing Principal is participating or has agreed to participate prior to notice of withdrawal or notice of change to Subscriber status, but such obligation shall exclude the cost of any Capital Cost Recovery Charges. Such obligation shall be reduced to the extent new Principals or Subscribers are allocated these costs that would otherwise have been chargeable to the departing Principal. After recouping such costs, the Executive Board may authorize reimbursement to the remaining Principals and Subscribers based on a depreciated value of the withdrawing or converting Principal's contribution.

c. Rights of departing Principal. Departing Principals shall have rights to copies of all data held by the PORTAL AGENCY relating to that Principal's Taxpayers and Licensee and other data relating specifically to the Principal.

d. The termination and/or withdrawal of a Principal shall not discharge or relieve any Principal of its obligations to the PORTAL AGENCY or other Participating Cities.

SECTION 18. AMENDMENT OF AGREEMENT.

This Agreement may be amended upon approval of a Supermajority Vote of the Executive Board except that any amendment affecting the following shall require consent of the legislative authorities of all Principals:

a. Expansion of the scope of services provided by the PORTAL AGENCY beyond the scope of expansion authorized in Section 5.c.
b. The terms and conditions of membership on the Executive Board.
c. Voting rights of Executive Board Members.
d. Powers of the Executive Board.
e. Principal contribution responsibilities.
f. Hold harmless and indemnification requirements.
g. Provisions regarding duration, termination or withdrawal.
h. The conditions of this Section.

This section shall not be construed to require legislative authority consent for the addition of a new Principal or agreement to serve an additional Subscriber, or to expand or contract the services purchased by any Principal or Subscriber or offered by the PORTAL AGENCY.

SECTION 19. TERMINATION OF AGREEMENT; DISSOLUTION OF AGENCY.

a. Generally. This Agreement may be terminated upon the approval of a Supermajority Vote of the Executive Board. The termination shall be by direction of the Executive Board to wind up business by a date specified by the Executive Board, which date shall be at least one (1) year following the date of the vote to terminate. Upon the final termination date, this Agreement shall be fully terminated.

b. Distribution of Property on Termination of Agreement. Upon termination of this Agreement, all property acquired during the life of the Agreement remaining in ownership of PORTAL AGENCY shall be disposed of in the following manner:

i. Real or Personal Property. All real or personal property purchased pursuant to this Agreement and all unexpended funds or reserve funds, net of all outstanding PORTAL AGENCY liabilities, shall be distributed to those Principals still participating in the PORTAL AGENCY on the day prior to the termination date and shall be apportioned between Principals based on the ratio that the average of each Principals' contributions to the operating budget over the preceding five (5) years bears to the total of all then remaining Principals' user fees paid during such five-year period. The Executive Board shall have the discretion to allocate the real or personal

property and funds as it deems appropriate, and the apportionment, determined consistent with the preceding sentence, need not be exact.

ii. Intellectual Property Rights. The Vendor will own, or have rights to, all its intellectual property per the terms of the Portal Services Contract, including the right to license the Portal operating system exclusively to the PORTAL AGENCY, its Principals and Subscribers. The Portal license rights, and all rights granted relating thereto, terminate with the termination of the Portal Services Contract. Notwithstanding this termination, the Principals and Subscribers shall retain the right after termination of the Portal license rights to acquire any and all information and data, including but not limited to Taxpayer, Licensee and their respective City data, then currently held by the Vendor or the PORTAL AGENCY. Upon termination of the Portal Development and Services Contract or the dissolution of the PORTAL AGENCY, any and all intellectual property owned by the PORTAL AGENCY (which excludes the Portal and any other intellectual property owned by the Vendor) will be transferred in its entirety to Principal with the largest Population. If said Principal does not agree to accept the intellectual property owned by the PORTAL AGENCY, it shall then be transferred in its entirety to the Principal with the next largest population, and so on should that Principal not agree to accept the intellectual property. If no Principal agrees to accept the intellectual property, then the Executive Board will attempt to sell the intellectual property at fair market value and distribute the proceeds in proper proportion to the current Principals in accordance with Subsection 19.b.i.

iii. Loaned Property. In the event of dissolution or termination of the PORTAL AGENCY, assigned or loaned assets shall be returned to the lending entity.

iv. Allocation of Liabilities. In the event outstanding liabilities of the PORTAL AGENCY exceed the value of personal and real property and funds on hand, all Principals shall contribute to retirement of those liabilities in the same manner as which they would share in the distribution of properties and funds.

c. ~~Notwithstanding~~ the foregoing, the Agreement may not be terminated if to do so would abrogate or otherwise impair any outstanding obligations of the PORTAL AGENCY, unless provision is made for those obligations.

SECTION 20. DISPUTE RESOLUTION.

a. Whenever any dispute arises between a Principal or the Principals or between the Principals and the PORTAL AGENCY (referred to collectively in this section as the "parties")

under this Agreement, which is not resolved by routine meetings or communications, the parties agree to seek resolution of such dispute by the process described in this section, which shall also be binding on Subscribers**.**

b. The parties shall seek in good faith to resolve any such dispute or concern by meeting, as soon as feasible. The meeting shall include the Chair of the Executive Board, the Manager, and a representative(s) of the Principal(s), if a Principal(s) is involved in the dispute, and/or a person designated by the Subscriber(s), if a Subscriber(s) is involved in the dispute.

c. If the parties do not come to an agreement on the dispute or concern, any party may request mediation through a process to be mutually agreed to in good faith between the parties within 30 days, which may include binding or nonbinding decisions or recommendations (whichever is mutually agreed to). The mediator(s) shall be mutually agreed upon and shall be skilled in the legal and business aspects of the subject matter of this Agreement. The parties shall share equally the costs of mediation and assume their own costs.

SECTION 21. INSURANCE.

The Executive Board, Manager, and Operations Board shall take such steps as are reasonably practicable to minimize the liability of the Participating Cities, including but not limited to the utilization of sound business practice. The Executive Board shall determine which, if any, insurance policies may be reasonably practicably acquired to cover the operations of the Portal Agency and the activities of the Parties pursuant to this Agreement (which may include Directors and Officers, Commercial General Liability, Auto, Workers' Compensation, Stop Gap/Employer's Liability, errors and omissions, crime/ fidelity insurance, CyberRisk), and shall direct the acquisition of same. [

SECTION 22. INDEMNIFICATION AND HOLD HARMLESS.

Each Principal shall indemnify and hold other Principals, their officers, officials, employees, agents and volunteers harmless from any and all claims, injuries, damages, losses or suits including attorney fees, arising out of that Principal's negligent acts or omissions in connection with the performance of its obligations under this Agreement, except to the extent the injuries or damages are caused by another Principal.

a. Each Principal shall indemnify and hold the PORTAL AGENCY and its officers, officials, employees and volunteers harmless from any and all claims, injuries, damages, losses or suits including attorney fees, arising out of that Principal's negligent acts or omissions in connection with the performance of its obligations under this Agreement, except to the extent the injuries and damages are caused by the PORTAL AGENCY.

b. As provided in its Articles of Incorporation, the PORTAL AGENCY shall indemnify and hold each Principal its officers, officials, employees and volunteers harmless from any and all claims, injuries, damages, losses or suits including attorney fees, arising out of the PORTAL AGENCY'S acts or omissions in connection with the performance of its obligations under this Agreement, except to the extent the injuries and damages are caused by any Principal.

c. Subscribers shall be required to agree to indemnify and hold harmless each Principal and the Portal Agency, their officers, officials, employees and volunteers from any and all claims, injuries, damages, losses or suits including attorney fees, arising out of Subscribers negligent acts or omissions in connection with its use of the Portal. To such degree as the Executive Board determines to be reasonable, appropriate, and consistent with applicable law and to be in the best interests of the Portal Agency, the Portal Agency may also indemnify and hold harmless Subscribers.

d. Should a court of competent jurisdiction determine that this Agreement is subject to RCW 4.24.115, then, in the event of liability for damages arising out of bodily injury to persons or damages to property caused by or resulting from the concurrent negligence of a party hereto and the PORTAL AGENCY, its officers, officials, employees, and volunteers, the party's liability hereunder shall be only to the extent of the party's negligence. It is further specifically and expressly understood that the indemnification provided in this Section constitutes the party's waiver of immunity under Industrial Insurance Title 51 RCW, solely for the purpose of this indemnification. This waiver has been mutually negotiated by the parties. The provisions of this section shall survive the expiration or termination of this Agreement.

e. Each party shall give the other parties proper notice as provided in Section 24, of any claim or suit coming within the purview of these indemnities. Termination of this Agreement, a Principal's withdrawal from the PORTAL AGENCY, or a Principal's conversion to Subscriber status (collectively for purposes of this subparagraph "Termination"), shall not affect the continuing obligations of each of the parties as indemnitors hereunder with respect to those indemnities and which shall have occurred prior to such Termination.

SECTION 23. INTERGOVERNMENTAL COOPERATION.

The PORTAL AGENCY shall cooperate with local, state and federal governmental agencies in order to maximize the utilization of any grant funds for equipment and operations and to enhance the effectiveness of the PORTAL AGENCY's operations and minimize costs of service delivery.

SECTION 24. NOTICE.

Notices required to be given to the PORTAL AGENCY under the terms of this Agreement shall be directed to the following unless all Principals are otherwise notified in writing:

Chair, PORTAL AGENCY Executive Board
c/o his/her Principal agency's address

Notices to Principals or Subscribers, Board Members or Representatives required hereunder may be given by mail, overnight delivery, facsimile or email (with confirmation of transmission), telegram, or personal delivery. Each Principal shall provide the Chair of the PORTAL AGENCY Executive Board written notice of the address for providing notice to said Principal. Any Principal wishing to change its mail or email address shall promptly notify the Chair of the Executive Board. Notice or other written communication shall be deemed to be delivered at the time when the same is postmarked in the mail or overnight delivery services, sent by facsimile or email (with confirmation of transmission), sent by telegram, or received by personal delivery.

SECTION 25. VENUE.

The venue for any action related to this Agreement shall be in the Superior Court in and for King County, Washington at Seattle, or if applicable, in Federal District Court, Western District of Washington.

SECTION 26. FILING.

As provided by RCW 39.34.040, this Agreement shall be filed prior to its entry in force with the King County Department of Executive Services Division of Records and Licensing Services, or its successor, Records and Elections, or, alternatively, listed by subject on a Principal's web site or other electronically retrievable public source.

SECTION 27. NO THIRD-PARTY BENEFICIARIES.

There are no third-party beneficiaries to this Agreement. No person or entity other than a party to this Agreement shall have any rights hereunder or any authority to enforce its provisions, and any such rights or enforcement must be consistent with and subject to the terms of this Agreement.

SECTION 28. SEVERABILITY.

The invalidity or any clause, sentence, paragraph, subdivision, section or portion of this agreement shall not affect the validity of the remainder of the Agreement.

SECTION 29. RATIFICATION.
All prior acts taken by the Principals and the PORTAL AGENCY consistent with this Agreement are hereby ratified and confirmed.

SECTION 30. EXECUTION, COUNTERPARTS AND EFFECTIVE DATE.

This Agreement and any amendments thereto, shall be executed on behalf of each Principal by its duly authorized representative and pursuant to an appropriate motion, resolution or ordinance. This Agreement may be executed in any number of counterparts, each of which shall be an original, but those counterparts will constitute one and the same instrument. This Agreement shall be deemed adopted and effective as of March 1, 2014, subject to prior approval by the legislative bodies of all four Original Principals, execution by each Original Principal, and prior filing of same as required by Section 26.

//
//
(Remainder of page left blank intentionally)
//
//
//
//

IN WITNESS WHEREOF, this Agreement has been executed by each party on the dates set forth below.

City of Bellevue

_____
City Manager

_____
Date

Approved as to Form:

_____
City Attorney

_____
Date

City of Everett

_____
Mayor

_____
Date

Approved as to Form:

_____
City Attorney

_____
Date

The City of Seattle

_____
Mayor

_____
Date

Approved as to Form:

_____
City Attorney

_____
Date

City of Tacoma

_____
City Manager

_____
Date

Approved as to Form:

_____
City Attorney

_____
Date

IN WITNESS WHEREOF, this Agreement has been executed by each pa1iy on the dates set fo1i h below.

City of Bellevue

City Manager
1-31-14

Date
Approved as to Form:

Date

The City of Seattle

Mayor

Date

Approved as to Form:

City Attorney

Date

City of Everett

Mayor

Date
Approved as to Form:

City Attorney

Date

City of Tacoma

City Manager

Date

Approved as to Form:

City Attorney

Date

IN WITNESS WHEREOF, this Agreement has been executed by each party on the dates set forth below.

City of Bellevue

_____

City Manager

_____

Date

Approved as to Form:

_____

City Attorney

_____

Date

City of Everett

Ray Stephanson

Mayor

1-29-2014

Attest: Sharon Fuller
City Clerk

Date

Approved as to Form: Jan Drago

City Attorney

1/27/14

Date

The City of Seattle

_____

Mayor

_____

Date

Approved as to Form:

_____

City Attorney

Date

City of Tacoma

_____

City Manager

_____

Date

Approved as to Form:

_____

City Attorney

Date

IN WITNESS WHEREOF, this Agreement has been executed by each party on the dates set forth below.

City of Bellevue

City Manager

Date

Approved as to Form:

City Attorney

Date

City of Everett

Mayor

Date

Approved as to Form:

City Attorney

Date

The City of Seattle

Mayor

Date

Approved as to Form:

of, City Attorney

Date

City of Tacoma

City Manager

Date

Approved as to Form:

City Attorney

Date

IN WITNESS WHEREOF, this Agreement has been executed by each party on the dates set forth below.

City of Bellevue

City Manager

Date

Approved as to Form:

City Attorney

Date

The City of Seattle

Mayor

Date

Approved as to Form:

City Attorney

Date

City of Everett

Mayor

Date

Approved as to Fonn:

City Attorney

Date

City of Tacoma

City Manager

12/19/2013

Date

Approved as to Form:

Debra Casper Deputy

1.:J.- 13-/3

Dat

12-18-2013

Andy Cherullo Date
Director of Finance

Attest:

.....

Doris Sorum
City Clerk

} - 3 0 13

Date

v. 11.5. I J

ORIGINAL

List of Exhibits

A. Proposed 2014 PORTAL AGENCY BUDGET SUMMARY (including number of Transactions used for cost allocation as between Original Principals)

B. 2015-2020 Estimated PORTAL AGENCY Operating Budget Summary

C. Capital Cost Recovery Charges

D. Calculation of New Participant Capped Cost Increment and New Participant Labor Cost Increment

Implementation Project costs funded by Seattle. This budget estimates also assumes only four cities participate in 2014.

Transaction Counts Calculations used for Cost Allocation as between Original Principals

Transaction Counts	Based on 2012 actual business license filings, business and occupations and gross receipts tax filings for each Original Principal				
	Seattle	**Bellevue**	**Tacoma**	**Everes t t**	**Total**
Transactions	212,457	30,927	50,000	14,392	307,776
% Allocation	69%	10%	16%	5%	100%

Exhibit B:

Multi-City Business License and Tax Portal Agency
2015-2020 Estimated Operating Budget Summary

This budget is an estimated six-year budget and assumes only four cities participating.

	2015	2016	2017	2018	2019	2020
Labor Total[8]	314,740	324,182	333,908	343,925	354,243	364,870
Contracts Total[9]	55,188	56,402	57,643	58,911	60,207	61,532
Overhead Total[10]	15,330	15,667	16,012	16,364	16,724	17,092
Vendor Total[11]	344,888	383,360	421,832	460,304	479,540	498,776
Operating Reserve - 15%	53,668	7,420	7,467	7,516	4,681	4,733
Total Estimated Budget	783,814	787,031	836,862	887,021	915,396	947,003
Estimated User Fee Revenue[12]	193,510	241,888	290,266	338,643	362,832	387,021
Estimated City Cost Allocation Revenues[13]	602,057	555,622	557,306	559,322	563,749	571,414
City of Seattle[14]	415,419	383,379	384,541	385,932	388,987	394,276
City of Bellevue	60,206	55,562	55,731	55,932	56,375	57,141
City of Tacoma	96,329	88,900	89,169	89,492	90,200	91,426
City of Everett	30,103	27,781	27,865	27,966	28,187	28,571

[8] This budget includes 2.5 FTE: the Portal Manager, a half-time administrative assistant and a full-time IT Project Manager/Business Analyst. The personnel for these positions will be provided by the City of Seattle and the costs in this budget include the fully-funded (salary, benefits, etc.) labor costs for all 2.5 positions. A separate loaned staffing agreement will be entered into between the Portal Agency and the City of Seattle in 2014 for these staff.

[9] Includes contracts for outside services such as Accounting, Insurance, Bank and the State Auditor.

[10] Funding for miscellaneous overhead items such as legal fees, office and operating supplies, printing and licenses/memberships.

[11] Includes costs estimated payable to-Gov Systems under the Portal Services Contract in 2014, from and after the Portal goes "live." e-Gov Systems will charge the Portal Agency $1.25 every time a business or taxpayer makes an online Portal filing, whether or not tax is owing. This per-filing cost is fixed for the first five years of Portal operation.

[12] Assumes the Executive Board approves a proposed user fee of $4 per online session per City (the proposed fee would be payable only when tax is owed; multiple tax and/or license filings on the same session would incur only one fee). This user fee is based on an estimated Portal use adoption rate by business and taxpayers of 15%. This adoption rate is expected to grow considerably each year.

[13] Cost Allocations are based on the 2012 Transaction count for each Original Principal, shown in Table 2.

[14] Excludes Seattle's contributions to start-up costs in 2014. Also excludes labor and operating costs for which Seattle will be reimbursed from the Total Budget shown above, per the loaned staffing agreement.

Transaction Counts Calculations used for Cost Allocation as between Original Principals

Transaction Counts	Based on 2012 actual business license filings, business and occupations and gross receipts tax filings for each Original Principal				
	Seattle	**Bellevue**	**Tacoma**	**Everet t**	**Total**
Transactions	212,457	30,927	50,000	14,392	307,776
% Allocation	69%	10%	16%	5%	100%

Estimated Adoption Rates

e-Gov Systems Recommended Adoption Rate	This is the recommended rate of adoption from e-Gov systems based on previous implementations.					
	2015	**2016**	**2017**	**2018**	**2019**	**2020**
Adoption Rate	40%	50%	60%	70%	75%	80%

CPI-U Rates Forecast

	2014	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**
CPI-U Forecast (Bellevue)	2.20%	2.20%	2.20%	2.30%	2.30%	2.30%	2.30%

Exhibit C

Capital Cost Recovery Charges

Beginning in 2015, every Participating City other than the City of Seattle will pay a yearly Capital Cost Recovery Charge to the Portal Agency which in turn will remit the annual total of such Charges paid to the City of Seattle. The Charges will remain in place until the total amount of $1,400,000 has been remitted to Seattle.

The Executive Board shall determine the timing for payment of the Capital Cost Recovery Charges.

Each Participating City's Capital Cost Recovery Charge will be determined based on the number of Transactions allocated to such City in the budget year in which the Charge will be collected, and in accordance with the following table:

Category:	**Smallest City**	**Smaller City**	**Small City**	**Medium City**	**Large City**
Transaction Count allocated to the City in the budget year	< 1000	1001 - 4000	4,001 to 14,400	14,401 to 31,000	>31,001
Capital Cost Recovery Charge payable annually	**$500**	**$1000**	**$2000**	**$4000**	**$6000**

Exhibit D

Calculation of New Participant Capped Cost Increment and New Participant Labor Cost Increment

New Participant Capped Cost Increment.

The New Participant Capped Cost Increment is an amount calculated in the development of each budget (or budget amendment) to identify the maximum amount by which Capped Costs may increase in the budget period *without requiring unanimous consent of the Executive Board Members representing all four Original Principals*. The Increment is determined by identifying the "CPI-U Limit for Capped Costs per Transaction" for the applicable budget period, assuming the Portal Agency has the same number of Participating Cities as the prior budget period and the Capped Costs from the previous period are inflated by the CPI-U Limit. The Capped Cost per Transaction is then multiplied by the number of Transactions attributable to new Participating Cities joining the Portal Agency in the budget period, and the resulting total is the maximum amount by which the Capped Costs in the new budget period may be increased over and above the Status Quo Capped Cost *without requiring unanimous consent*.

Illustration: **Calculation of New Member Capped Cost Increment for Year X** *Assuming: 1-year budget period; addition of 2 member cities proposed in Year X*	
Part 1: Calculating CPI-U Limit for Capped Costs Per Transaction	
CPI-U Limit for Capped Cost for Year X, • Inflate Capped Costs for the previous year by the CPI-U Limit.	$16,000
Estimated Transaction Count for Year X from currently Participating Cities • Includes all Cities participating as Principals or Subscribers in the previous year. • Transaction count is that used for purposes of estimating the cost allocations of these Participating Cities in Year X.	125,000
Capped Cost Per Transaction ($16,000 ÷ 125,000)	**$0.128**
Part 2: Calculating New Member Capped Cost Increment	
New Member Transaction Count • Total Transactions assigned to the 2 new Participating Cities for purposes of budget allocation in Year X	10,000
New Member Capped Cost Increment for Year X ($0.13 x 10,000)	**$1,280**
Capped Costs in Year X may be increased by Supermajority Vote to a level of $17,280. Capped Costs in excess of that amount would require Supermajority Vote and unanimous approval by Board Members representing the Original Principals.	

New Member Participant Labor Cost Increment.

The New Participant Labor Cost Increment is an amount calculated in the development of each budget (or budget amendment) to identify the maximum amount by which Labor Costs may increase in the budget period *without requiring unanimous consent of the Executive Board Members representing all four Original Principals*. The Increment is determined by identifying the "Status Quo Labor Cost per Transaction" for the applicable budget period, assuming the Portal Agency has the same number of Participating Cities and staff as the prior budget period. The Labor Cost per Transaction is then multiplied by the number of Transactions attributable to new Participating Cities joining the Portal Agency in the budget period, and the resulting total is the maximum amount by which the Labor Costs in the new budget period may be increased over and above the Status Quo Labor Cost *without requiring unanimous consent*.

Illustration: **Calculation of New Participant Labor Cost Increment for Year X** *Assuming: 1-year budget period; addition of 2 member cities proposed in Year X*	
Part 1: Labor Cost Per Transaction	
Status Quo Labor Costs for Year X • Assuming same number of staff (including employees, if any, and loaned staff) as were engaged by the Portal Agency in the previous year, and adding any estimated increases in costs of salary, benefits, etc. for those same personnel over and above the previous year's costs.	$350,000
Estimated Transaction Count for Year X from Currently Participating Cities • Includes all Cities participating as Principals or Subscribers in the previous year. • Transaction count is that used for purposes of estimating the cost allocations of these Participating Cities in Year X.	125,000
Labor Cost Per Transaction ($350,000 ÷ 125,000)	**$2.80**
Part 2: New Participant Labor Cost Increment	
New Participant Transaction Count • Total Transactions assigned to the 2 new Participating Cities for purposes of budget allocation in Year X	10,000
New Participant Labor Cost Increment for Year X ($2.80 x 10,000)	**$28,000**
*Labor Costs in Year X may be increased by Supermajority Vote to a level of $378,000. Labor Costs in excess of that amount would require Supermajority Vote **and** unanimous approval by Board Members representing the Original Principals.*	



BYLAWS

APPENDIX NO. A3

BYLAWS

OF

WASHINGTON MULTI-CITY BUSINESS LICENSE AND TAX PORTAL AGENCY

("PORTAL AGENCY")

ARTICLE I. PURPOSES

As set forth in the Washington Multi-City Business License and Tax Portal Agency Interlocal Agreement dated as of March 1, 2014, by and between the Cities of Bellevue, Everett, Seattle and Tacoma (the "Agreement"), the PORTAL AGENCY is organized in accordance with the Interlocal Cooperation Act (Chapter 39.34 RCW) and the Nonprofit Miscellaneous and Mutual Corporations Act (Chapter 24.06 RCW) as a public body and instrumentality of its members to jointly exercise essential governmental functions of its members.

ARTICLE II. DEFINITIONS; CONFLICTING PROVISIONS

All capitalized terms used and not otherwise defined in the Bylaws shall have the meaning set forth in the Agreement. In the event of a conflict between a provision of the Bylaws and a provision of the Agreement, the provision of the Agreement shall prevail.

ARTICLE III. OFFICES

The principal office and place of business of the PORTAL AGENCY in the state of Washington shall be initially located at Seattle City Hall, 600 4th Avenue, Seattle, WA 98104. The name and address of its initial registered agent is Glen Lee, Finance Director, City of Seattle, 700 Fifth Avenue, Suite 4350, Seattle, WA 98104.

ARTICLE IV. BOARD

Section 4.1. General Powers. The business and affairs of the PORTAL AGENCY shall be managed by its Executive Board (referred to in these Bylaws as either the "Executive Board" or "Board"), which shall be deemed a "Board of Directors" as that term is used in RCW 24.06.125. In addition to its other powers and authority set forth in the Agreement and subject to

applicable law, the terms of the Agreement or the terms of any gift, devise, bequest or other transfer, the Board shall have the full power, in its sole discretion, to change the form of any investment and, for that or other purpose of the PORTAL AGENCY, to dispose of any property held by the PORTAL AGENCY. The Board shall have the right to employ or retain persons or entities to carry out the purposes of the PORTAL AGENCY, including but not limited to attorneys, consultants, engineers, contractors and accountants.

Section 4.2 Composition of Board. The Board of the PORTAL AGENCY shall consist of one individual representative from each member entity ("Principal" as that term is defined in the Agreement), except as shared representation of Principals may be required by terms of Section 7.c of the Agreement. In addition, from and after such time as the PORTAL AGENCY has at least one Subscriber, there shall be one (1) non-voting Board Member representing Subscribers. Each representative is a "director" as that term is used in RCW 24.06.130, and is referred to in the Agreement as a "Board Member" and in these Bylaws as a "Board Member." Board Members representing a single Principal or Subscriber agency shall not have terms but rather each such Board Member shall serve at the pleasure of the agency that the Board Member represents. Board Members representing multiple Principals or Subscribers shall be elected biennially in accordance with Section 7.d of the Agreement. In order to serve as a Board Member, an individual must be the Chief Financial Officer (CFO) or deputy or equivalent of the represented agency (or the CFO, deputy or equivalent of one of the represented Principals or Subscribers, in the case of a Board Member representing multiple Principals or Subscribers).

Section 4.3 Designation and Qualifications of Alternates. Each member of the Executive Board shall designate in writing an alternate who shall serve as a member of the Executive Board during his or her absence or unavailability to serve, and in such case the alternate shall have the full rights and privileges of the absent member. Alternates must meet the same qualifications as the designated Board member or have similar financial expertise and be in a management position within their City. All written designations shall become effective upon delivery to the Chair of the Executive Board and shall remain in effect until revoked in writing by the designating member(s). In the event of any question of authority to act as an alternate, the determination of the Chair based upon the records on file with the Chair shall be determinative.

Section 4.4 Tenure. Unless the Board Member resigns or is removed in accordance with these Bylaws, each Board Member shall hold office until replaced by resolution or written motion of the legislative body of the appointing Principal. Notwithstanding the foregoing, no Board Member shall continue in that capacity if he or she no longer holds a position that qualifies him or her for the seat, and Board Members representing multiple Principals or

Subscribers shall be re-appointed every biennium consistent with the terms of Section 7.d of the Agreement.

Section 4.5 Annual and Regular Meetings. The annual meeting of the PORTAL AGENCY shall be held in March of each year, at such time and place as may be determined by the Executive Board, for the transaction of such business as may come before the meeting. The Executive Board may specify by resolution the time and place for holding any other regular Board meetings and notice for such meetings shall be given as required by the Agreement. Not less than fourteen (14) days advance notice shall be given of regular meetings.

Section 4.6 Special Meetings. Special meetings of the Board may be called by the Chair or by the written request of not less than two Executive Board Members, upon giving all other Board Members not less than ten (10) days prior notice. Notice of special meetings of the Board stating the date, time and place thereof shall be delivered to Board Members in accordance with RCW 24.06.104, as it may be amended and as otherwise required by the Agreement. The notice must be written or by electronic means. Notice shall also be given to any other persons as may be required by the Open Public Meetings Act (Chap. 42.30 RCW) and other applicable law. In an emergency, the Executive Board may dispense with written notice requirements for special meetings but must in good faith implement best efforts to provide fair and reasonable notice to all Executive Board meetings.

Section 4.7 Matters Requiring Notice. Prior written notice meeting the requirements of notice for special meetings shall be required in the case of action on any of the following matters:

A. All elections of the Chair or the recall of the Chair;
B. Budget approval and amendments;
C. Dues and assessments;
D. All final action on any commitment to an expenditure not authorized by an approved budget;
E. Contractual commitments requiring expenditures not previously authorized;
F. Changes in the Bylaws of PORTAL AGENCY;
G. Changes in membership; and
H. Reversal or modification of Executive Board decisions or modification of Executive Board authority or duties.

Section 4.8 Waiver of Notice of Special Meeting. Whenever any notice is required to be given to any Board Member pursuant to applicable law, a waiver in writing signed by the Board Member, entitled to notice, shall be deemed equivalent to the giving of notice. Any Board Member may waive notice of any meeting at any time. The attendance of a Board Member at a

meeting shall constitute a waiver of notice of the meeting except where a Board Member attends a meeting for the express purpose of objecting to the transaction of any business because the meeting is not lawfully convened. Unless otherwise required by law, neither the business to be transacted at, nor the purpose of, any regular or special meeting of the Board need to be specified in the notice or waiver of notice of such meeting.

Section 4.9 Quorum. A simple majority of the Members (or their alternates) in number (excluding any Member which per the Agreement has given notice of withdrawal or which has been terminated by voted of the Executive Board) shall constitute a quorum of the Executive Board for purposes of doing business at any time. Members may attend meetings by telephone conference or equivalent means of voice communication.

Section 4.10 Manner of Acting; Rules of Order. The Board shall strive to operate by consensus. All Board decisions on items not listed in Section 7.k of the Agreement or as otherwise specified in Sections 16, 18 and 19 of the Agreement, require a Simple Majority Vote for approval. A Member may not split her or her vote on an issue. No voting by proxies or mail-in ballots will be allowed. Unless otherwise approved by vote of the Executive Board, upon the request of any Member of the Executive Board, Robert's Revised Rules of Order shall govern any proceeding of the Executive Board. The Board may act by voice votes called for by the Chair, but any Member may require a recorded tabulation of votes by making a request either immediately before the vote is taken or immediately after a voice vote is taken.

Section 4.11 Supermajority Voting. Supermajority Voting shall be required on those items listed in Section 7.k of the Agreement. A "Supermajority Vote' means Executive Board approval of an item accomplished by securing affirmative votes of not less than sixty-six percent (66%) of all voting Board Members of the Executive Board in number, and not less than sixty-six percent (66%) in number of the Original Principals (the Cities of Bellevue, Everett, Seattle and Tacoma).

Section 4.12 Advisory and Board Committees. In addition to the Tax and Finance Operations Committee ("Operations Committee") established by the Agreement, and subject to the terms of the Agreement, the Executive Board may create other special advisory committees as it deems appropriate, and members of such advisory committees shall be appointed by the Executive Board. Persons who serve as members of any advisory committee are not be required to be Board Members or elected officials. The Board also may create standing or special committees of the Executive Board. Chairpersons and other members of standing committees or special committees (which excludes the Operations Committee) shall be Board Members or alternate Board Members and shall be designated by the Board, except that the Treasurer shall chair any Finance Committee. The Board shall attempt to appoint committee members in a manner that encourages diversity of representation on committees that reflects the diversity among Members. Committees shall be governed by the same rules regarding

meetings, action without meetings, notice, waiver of notice, and quorum (but not voting requirements) as applied to the Board; *provided that* meetings of the Operations Committee shall require such notice as required per Article VI, Section 6.8. The designation of any standing or special committee and the delegation to them of any authority shall not relieve the Board, or any Board Members of any responsibility imposed by law. No committee shall have the authority to take any action inconsistent with the Agreement, the Bylaws, or RCW 24.06.145.

Section 4.13 Agendas. Prior to each Executive Board meeting the Chair shall establish an agenda for the meeting. At the beginning of the meeting, any Board member may request that an item be added to the agenda, provided that, items requiring prior notice (See Section 4.7) shall not be so added unless all Board members are present and waive the requirement of notice and agree to entertain the action.

Section 4.14 Open Public Meetings. All meetings of the Board shall be open to the public as and to the extent required by the Agreement, the Open Public Meetings Act (Chap. 42.30 RCW) and other applicable law.

Section 4.15 Resignation; Removal. A Board member may be removed by the appointing agency (or agencies in the case of a Board member representing multiple Principals or Subscribers) which he or she represents, and an individual Board Member may personally resign at any time. Resignation shall be effective upon the Board Member or the appointing agency(s) delivering written notice to the Chair or, if the Chair is resigning, to the Vice-Chair.

Section 4.16 Vacancies. Any vacancy occurring in the Board shall be filled by the appropriate appointing agency or agencies (in event the Member represents multiple Principals or Subscribers).

Section 4.17. Compensation. All Board Members and their alternates shall serve without compensation; however, the PORTAL AGENCY may pay for or reimburse Executive Board Members and alternates for out-of-pocket costs related to service on the Executive Board.

ARTICLE V. OFFICERS

Section 5.1 Number. The PORTAL AGENCY shall have a Chair and a Vice-Chair, each of whom shall be elected by the Board. The Board shall also elect a Secretary and Treasurer or shall appoint same if non-Board Members are to fill these positions. Such other officers and assistant officers, as set forth in this Section 5.1 or as may be deemed necessary or appropriate may be appointed by the Board. The Chair shall preside at all meetings of the Executive Board

and shall have the additional responsibilities described in Section 5.4. The Vice-Chair shall serve as the Treasurer and Secretary of the Corporation during any times that a separate Treasurer or Secretary have not been appointed by the Board consistent with Section 7.l of the Agreement. Any two or more offices may be held by the same person, with the exception that the Chair and Vice-Chair, the Chair and Treasurer, or the Chair and Secretary may not be held by the same person.

Section 5.2 Election and Term of Office. The Chair and Vice-Chair initially shall be elected by Simple Majority Vote of the Board Members and shall serve through April 1, 2016, whereupon a new Chair and Vice-Chair shall be elected by the Board for a two-year term. Biennially thereafter, the Board shall elect a new Chair and Vice-Chair for two-year terms commencing each April 1. In the event of a vacancy in the Chair position, the Vice-Chair shall assume the Chair for the balance of the term of the departed Chair. In the event of a vacancy in the Vice-Chair position, the Executive Board shall elect a new Vice-Chair to serve the balance of the term of the departed Vice Chair. If the Treasurer and Secretary Officer positions are to be filled by Board Members, these positions shall be elected at the same time as the election of the Chair and Vice-Chair.

Section 5.3 Resignation. Any officer may resign at any time by delivering written notice to the Chair or by giving oral notice at any meeting of the Board. Any such resignation shall take effect at the time specified in the notice or, if the time is not specified, upon delivery of the resignation. Unless otherwise specified in the notice, the acceptance of a resignation shall not be necessary to make it effective.

Section 5.4 Chair (President). The Chair of the Executive Board (who shall be "President" under RCW 24.06.144 and for any required purposes) shall preside at all meetings of the Board and shall exercise and perform such other powers and duties enumerated below, and as may be determined from time to time by resolution of the Board. The Chair shall:

A. Preside at regular and special meetings and may call regular and special meetings of the Executive Board;
B. Select the site and agenda for all meetings;
C. Arrange for preparation and mailing or delivery of all meeting notices to Board member;
D. Arrange the maintenance and circulation of minutes of the meetings of the Board;
E. Act as the spokesperson for PORTAL AGENCY;
F. Execute documents on behalf of the Executive Board; and
G. Such other duties as identified in the Agreement and as may be delegated from time to time by the Executive Board.

In the absence of the Chair, or if there be none, the Vice-Chair shall preside at all meetings of the Board. The Chair may sign deeds, leases, bonds, Agreements, or other instruments which the Board has authorized to be executed, except in cases where the signing or execution thereof shall be expressly delegated by the Board or by these Bylaws to some other officer or agent of PORTAL AGENCY or shall be required by law to be otherwise signed or executed. In general, the Chair shall perform all duties incident to office of Chair and such other duties as may be prescribed by resolution of the Board.

Section 5.6 Vice-Chair. The Vice-Chair shall perform the duties of the Chair in the absence of the Chair. When so acting, the Vice-Chair shall have all the powers of and be subject to all the restrictions upon such officers and shall perform such other duties as from time to time may be assigned to the Chair by resolution of the Board.

Section 5.7 Secretary. The Vice-Chair, serving as Secretary, or a separately appointed Secretary, shall keep or cause to be kept, the minutes of the proceedings of the Board; shall give notices in accordance with the provisions of these Bylaws and as required by law; shall be custodian of the corporate records of the PORTAL AGENCY; shall have charge and custody of and be responsible for maintaining or overseeing maintenance of correct and complete nonfinancial books and records of the PORTAL AGENCY. The Secretary shall perform such other duties as from time to time may be assigned by resolution of the Board. If a person who is not a Board Member is appointed as Secretary, he/she shall not be considered an *ex officio* member of the Board.

Section 5.8 Treasurer. The Vice-Chair serving as Treasurer, or a separately appointed Treasurer, shall be responsible for maintaining, or overseeing maintenance of, all financial records of the PORTAL AGENCY, assuring the appropriate handling of all revenues and expenditures, and shall assist the Board in preparation of the annual budget. The Treasurer shall maintain or oversee maintenance of complete books and records of account, for all funds and securities of the PORTAL AGENCY, the transfer of receipts for money due and payable to the PORTAL AGENCY from any source whatsoever, and the deposit of all such money in the name of the PORTAL AGENCY in the banks, trust companies or other depositories as shall be selected in accordance with law. The Treasurer in general shall perform all duties incident to the office of Treasurer and such other duties as from time to time may be assigned to the Treasurer by resolution of the Board. If required by the Board, the Treasurer shall give a bond for the faithful discharge if his or her duties, in such sum and with such surety or sureties as the Board shall determine. If a person who is not a Board Member is appointed as Treasurer, he/she shall not be considered an *ex officio* member of the Board.

Section 5.9 Assistant Officers. The assistant officers, if any are appointed by the Board, shall in general perform such duties as are customary or as shall be assigned to them by resolution of

the Board. If required by the Board, the assistant Treasurers shall respectively give bonds for the faithful discharge of their duties in such sums and with such sureties as the Board shall determine.

Section 5.10 Delegation. In the case of absence or inability to act of any officer and of any person authorized to act in his/her place, the Board, by resolution, may, from time to time, delegate the powers or duties of such officer to any other officer or any Board Member or other person whom it may select. The Chair, by written notice to the Board, may delegate duties or powers, in addition to those listed, to officers of PORTAL AGENCY as necessary or appropriate to the conduct of the affairs of PORTAL AGENCY.

Section 5.11 Vacancies. Vacancies in any office arising from any cause may be filled by the Board at any regular or special meeting of the Board subject to the notice provisions set forth in Section 4.4 through 4.16 of the Bylaws.

Section 5.12 Indemnification. The PORTAL AGENCY shall indemnify officers and Board Members as set forth in the Articles of Incorporation.

ARTICLE VI. OPERATIONS COMMITTEE

Section 6.1 Powers. The Tax and Finance Operations Committee ("Operations Committee") shall have such powers, as described in Section 9 of the Agreement. No compensation shall be paid by the PORTAL AGENCY for any service as a Representative on the Operations Committee or as its Chair.

Section 6.2 Membership. Membership of the Operations Committee shall include one (1) Representative from each Principal, appointed by that Principal from time to time, plus at least one (1) representative, appointed by the Executive Board, to represent Subscribers. Each Principal shall also appoint in writing a designated alternate to serve on the Operations Committee in case of absence of the primary Representative**.**

Section 6.3 Qualification to serve on Operations Committee. Representatives and their alternates shall be staff from the Principal they represent, with expertise in city tax policy and administration and/or city financial policy and administration. Persons serving on the Operations Committee are referred to as Representatives (or alternates) and shall serve without compensation from the PORTAL AGENCY.

Section 6.4 Operations Committee Officers. The Operations Committee shall select an Operations Committee Chair and Vice-Chair from among the membership of the Operations Committee. It will be the function of the Operations Committee Chair to preside at the

meetings of the Operations Committee, and the Operations Committee Vice-Chair shall assume this role in absence of the Operations Committee Chair. The officers shall be initially elected at the first meeting of the Operations Committee following the effective date of this Agreement, by majority vote of the Representatives on the Operations Committee and shall serve through March 2016. Thereafter, the Operations Committee shall biannually elect an Operations Committee Chair and Vice-Chair for two-year terms beginning each April 1. In the event of a vacancy in the Chair position, the Vice-Chair shall assume the Chair for the balance of the term of the departed Chair. In the event of a vacancy in the Vice-Chair position, the Operations Committee shall elect a new Vice-Chair to serve to the balance of the term of the departed Vice-Chair. An officer of the Operations Committee elected to fill the unexpired term of his or her predecessor shall not be precluded from serving one or more full annual terms of office following the end of such unexpired term.

Section 6.5 Quorum. A quorum at any meeting of the Operations Board shall consist of Representatives of the Operations Committee (or their alternates) representing a simple majority of all members of the Committee. Representatives may attend meetings by telephone conference or equivalent means of voice communication.

Section 6.6 Voting. All actions and recommendations of the Operations Committee shall be approved by majority vote of those present and voting. Each Representative shall have one vote. No proxy votes shall be allowed. There shall be no weighted voting.

Section 6.7 Staffing. The Operations Committee shall be staffed by the Portal Agency Manager and such additional agency staffing as the Manager may deem appropriate.

Section 6.8 Meetings. The Operations Committee shall meet not less than once every calendar quarter, at a time and place designated by the Chair of the Operations Committee or by a majority of its Representatives. Not less than ten (10) days advance notice of regular meetings shall be given. Special meetings may be called by the Chair of the Operations Committee or Representatives representing at least two or more members of the Committee representing at least two different Principals and upon giving all other Representatives not less than seven (7) days prior notice of such meeting. In an emergency, the Operations Committee may dispense written notice requirements for special meetings, but must, in good faith, implement best efforts to provide fair and reasonable notice to all Representatives. Representatives (or alternates) may participate in meetings by telephone conference or other equivalent means of voice communication.

Section 6.9 Additional Rules. The Operations Committee may adopt additional rules for its operations that are not inconsistent with the Agreement or these Bylaws.

ARTICLE VII. STAFF AND CONSULTANTS

The staff of PORTAL AGENCY shall consist of the Manager and such other staff positions established by the Board. The Board shall appoint the Manager, pursuant to the provisions of the Agreement. The Manager shall appoint persons to fill other staff positions, subject to such confirmation by the Board as the Board may require. Only the Board shall be authorized to hire or retain legal counsel and independent accountants and auditors. Other consultants may be designated in such manner as the Board may determine, subject to Sections 6 and 7 of the Agreement.

ARTICLE VIII. EXECUTION OF AGREEMENTS AND OTHER INSTRUMENTS

Execution of Agreements and Deeds. Except as otherwise provided by resolution of the Board authorizing the execution thereof, all agreements, deeds, leases, transfers and other written instruments binding upon the PORTAL AGENCY for amounts involving the expenditure of greater than $50,000, shall be executed on behalf of the PORTAL AGENCY by the Chair and one other officer. The execution of documents involving amounts less than $50,000 may be signed by the PORTAL AGENCY Manager alone, after advising the Board.

ARTICLE IX. FINANCES

Section 9.1 Loans. The PORTAL AGENCY is not authorized to issue debt. No loans shall be made by the PORTAL AGENCY to any officer, Board Member or private entity, nor shall loans be made in violation of the Washington State Constitution or applicable law.

Section 9.2 Checks, Drafts, Warrants, Orders and Credit Cards. All checks, drafts, warrants, credit cards, debit cards or other orders for the payment of money or issued in the name of the PORTAL AGENCY shall be signed by officers of the PORTAL AGENCY or the Manager subject to such limits and in the manner as shall from time to time be prescribed by resolution of the Board and consistent with law applicable to Washington State local government entities. In the absence of such provision by the Board such instrument shall be signed by any two officers of the PORTAL AGENCY, one of whom shall be the Vice-Chair. Use of credit cards by PORTAL AGENCY shall be in compliance with RCW 43.09.285.

Section 9.3 Contributions and Disbursements. All contributions and other funds received by PORTAL AGENCY shall be deposited in a special account or accounts in such banks, trust companies or other depositories as the Board may select. All disbursements shall be made under proper authority of the Board. All contributions, income to and disbursements of

PORTAL AGENCY shall be recorded by the Vice-Chair's (or Treasurer's) designee in appropriate books and records and such records shall be subject to examination at any reasonable time, upon request by any director.

Section 9.4 Budget/Financial Management. An annual budget of proposed receipts, operating income and expenditures shall be prepared by the Manager and submitted to the Board for its approval by May 1 prior to the beginning of the fiscal year in which that budget will take effect, and if not so timely submitted, the Vice-Chair (or Treasurer) shall submit a budget to the Board for its approval as soon as practicable after such date. The budget shall identify the level of rates and charges upon which revenue projects are based. When finally approved by the Board after action by Principals per the Agreement, such budget shall be the authorization for expenditures and operating expenses of the PORTAL AGENCY, subject to subsequent changes in such budget made by the Board.

Section 9.5 Expenditures for Qualifying Purposes Only. Subject to applicable law, the funds of the corporation may be expended or distributed only for the purposes of the PORTAL AGENCY as described in the Agreement and in the Articles of Incorporation.

ARTICLE X. ETHICS

The PORTAL AGENCY, its Board Members, committee members and employees (including loaned staff) shall be subject to and comply with the requirements of Ch. 42.23 RCW ("Code of Ethics for Municipal Officers – Contract Interests") as the same may be amended or replaced from time to time.

ARTICLE XI. SEAL

The PORTAL AGENCY need not have a corporate seal. If the Board adopts a corporate seal, the seal of the PORTAL AGENCY shall be circular in form and consist of the name of the Washington Multi-City Business License and Tax Portal Agency, the state and year of incorporation, and the words "Corporate Seal."

ARTICLE XII. BOOKS AND RECORDS

The PORTAL AGENCY shall keep correct and complete books and records of account, minutes of the proceedings of the Board, and any committees designated by the Board, and such other

records as may be necessary or advisable. All books and records shall be subject to disclosure under the Public Records Act, Chapter 42.56 RCW.

ARTICLE XIII. COPIES OF RESOLUTIONS

Any person dealing with the PORTAL AGENCY may rely upon a copy of any of the records of the proceedings, resolutions or votes of the Board when such records are certified by the Vice- Chair or Secretary, if a separate Secretary is appointed.

ARTICLE XIV. AMENDMENTS TO BYLAWS.

These Bylaws may be adopted, altered, amended or repealed, and new Bylaws may be adopted, all by Supermajority Vote of the Board.

The undersigned, being the Chair and Vice-Chair of the PORTAL AGENCY, hereby certified that these Bylaws are the Bylaws of the PORTAL AGENCY, adopted by Resolution No. 2014-_____of the Board on__, 2014.

Dated this____day of_____, 2014.

_____

_____

Chair

_____

_____

Vice-Chair

APPENDIX B: ORGANIZATIONAL CHART, ROSTER

Washington State Municipalities
Governing Board - Executive Board

City of Bellevue	Toni Call
City of Des Moines	Beth Anne Wroe
City of Everett	Susy Haugen
City of Lake Forest Park	Lindsey Vaughn
City of Renton	Jan Hawn
City of Seattle	Glen Lee
City of Tacoma	Andy Cherullo

Washington State Municipalities
Governing Positions

City of Seattle	Glen Lee	Chair
City of Tacoma	Andy Cherullo	Vice-Chair
Francis and Company	Horace Francis	Treasurer
FileLocal Agency	Julie Panick	Secretary

Washington State Municipalities
Governing Board - Executive Board Alternates

City of Bellevue	Jamie Robinson
City of Des Moines	Shawn Hunstock
City of Everett	Sharon Fuller
City of Lake Forest Park	Aurora Belli
City of Renton	Kari Roller
City of Seattle	Joseph Cunha
City of Tacoma	Susan Ramirez

Washington State Municipalities
Governing Board - Operations Committee

City of Bellevue	Troy Lucas
City of Des Moines	Shawn Hunstock
City of Everett	Anna Pankovich
City of Lake Forest Park	Lindsey Vaughn
City of Renton	Nate Malone
City of Seattle	Joseph Cunha
City of Tacoma	Danielle Larson

Washington State Municipalities
FileLocal Agency

Program Manager	Kevin Fitzpatrick
Project Manager	Wendy Thomaston
Program Assistant	Julie Panick

Washington State Municipalities
Technical Service Vendors

Software as a Service	Avenu Insights
Payment Processing	Kubra Data Transfer LTD.
Information Security	Leviathan Security Group

Washington State Municipalities
Professional Service Vendors

Accounting	Francis and Company
Legal	Madrona Law

FL2019-09 Attachment C

AUTHORITIES DELEGATED BY FILELOCAL EXECUTIVE BOARD	TOPIC	DOCUMENTATION	PROGRAM MANAGER	OPERATIONS COMMITTEE	OTHER	ACCOUNTANT	LEGAL
Authorizes budgeted expenditures of $50,000 or less - excluding Program Manager (PM) requests.	F	(FM §6.1)	X				
Authorizes budgeted expenditures of more than $50,000 - excluding PM requests .	F	(FM §6.1)			X		
Authorizes unbudgeted expenditures of $5,000 or less-excluding PM requests .	F	(FM §6.1)			X		
Authorizes unbudgeted expenditures of more than $5,000-excluding PM requests.	F	(FM §6.1)			X		
Contract Review >$5,000	F	(FM §6.1)			X		
Authorizes all budgeted PM requests $5,000 or less.	F	(FM §6.1)			X		
Authorizes all budgeted PM requests greater than $5,000.	F	(FM §6.1)			X		
Authorizes all unbudgeted PM requests $2,000 or less.	F	(FM §6.1)			X		
Authorizes all unbudgeted PM requests greater than $2,000.	F	(FM §6.1)			X		
Assist in Development and review proposed agency budgets	F	(FM §3)		X			
Advises on proposed budget	F	(FM §3)	X				
Develops proposed operating budget in consultation with operations committee	F	(FM §3)	X				
Submits budget and operation performance reports to Board	F	(FM §1)	X				
Reviews/approves cash disbursements	F	(FM, §6.2)	X				
Prepares checks, maintains and initiates electronic payments	F	(FM, §6.2)				X	
Reviews bank accounts and reconciliations	F	(FM, §6.2)				X	
Approves check requests (as authorized by Executive Board)	F	(FM, §6.3)				X	
Controls check stock	F	(FM, §6.4)				X	
Establishes and maintains accounting system	F	(FM, §2)				X	
Preparation of financial statements	F	(FM, §11)				X	
Provides external audit preparation and response	F	(FM, §6.11)				X	
Conducts compliance monitoring, financial analysis, internal audits, and other financial management and accounting services as directed by Board	F	(FM, §6.11)				X	

Legend	
F=Fiscal	ILA=Interlocal Agrement
O=Operations	B=Bylaws
P=Policy	SLA=Service Level Agreement
FM=Fiscal Manual	

FL2019-09 Attachment C

AUTHORITIES DELEGATED BY FILELOCAL EXECUTIVE BOARD	TOPIC	DOCUMENTATION	PROGRAM MANAGER	OPERATIONS COMMITTEE	OTHER	ACCOUNTANT	LEGAL
Provides legal services regarding formation as a non-profit municipal corporation	L	(FL2014-18)					X
Provides general legal counsel	L	(FL2014-18)					X
Manages/oversees vendor performance	O	(ILA §11)	X				
Consults with Operations Committee on issues coming before Board	O	(ILA §11)	X				
Provide, equip, and maintain office space for staff	O	(FL2014-19)			X COS		
Reviews and develops operations policy and amendments, new service options, and other matters directed by Board	P	(ILA §9)		X			
Reports and recommends on policy matters deemed appropriate	P	(ILA §9)		X			
Assists in communications to City Councils, legislators, business community, etc.	Policy	(ILA 16-17)		X			
Conducts outreach to tech staff within respective cities	Policy	(ILA 16-17)		X			
Briefs executive board members	Policy	(ILA 16-17)		X			
Administers day-to-day operations consistent with policies	Policy	(ILA 18)	X				
Conducts outreach to taxpayers, licenses and businesses	Policy	(ILA 18)	X				
Advise on conflicts of interest	Policy	(SLA, p4)			X SEEC		
Preserves agency public records as required by state law, response to public records requests, segregation of agency records from city records	Policy	(SLA, p5)	X		X Seattle		
Outreach and communications with elected officials	Policy				xOIR		
Appoints other staff positions established by Board	Staffing	(B p9)	X				
Appoints persons to fill other staff positions (Administrative support staff, project manager/business analyst, etc.)	Staffing	(ILA 18, SLA 3)	X				
Backfills employees	Staffing	(SLA, p4)			X Seattle		

Legend

F=Fiscal	ILA=Interlocal Agrement
O=Operations	B=Bylaws
P=Policy	SLA=Service Level Agreement
FM=Fiscal Manual	

Executive Board Meeting Schedule

Executive Board meeting schedules are approved via a resolution passed by the Board. All meetings are held at the Seattle Municipal Tower (SMT) and are open to the public.

Year	Type	Date	Time	Location
2020	Special	Feb 24, 2020	11:00am – 12:00pm	SMT 4090
	Regular	Mar 19, 2020	CANCELLED	SMT 4086
	Regular	Apr 17, 2020	11:00am – 12:00pm	Conference Call
	Regular	May 28, 2020	11:00am – 12:00pm	Conference Call
	Regular	Sep 30, 2020	11:00am – 12:00pm	Conference Call
	Regular	Dec 17, 2020	11:00am – 12:00pm	Conference Call
2019	Regular	Mar 28, 2019	11:00am – 12:00pm	SMT 4070
	Regular	May 30, 2019	11:00am – 12:00pm	SMT 4070
	Regular	Sept 26, 2019	11:00am – 12:000m	SMT 4070
	Regular	Dec 19, 2019,	11:00am – 12:00pm	SMT 4070
2018	Special	Mar 19, 2018	11:00 am – 12:00 pm	SMT 4240
	Annual	Mar 26, 2018	12:00 pm – 1:00 pm	SMT 4070
	Regular	May 29, 2018	12:00 pm – 1:00 pm	SMT 4090
	Regular	Sep 24, 2018	12:00 pm – 1:00 pm	SMT 4070
	Regular	Dec 10, 2018	12:00 pm – 1:00 pm	SMT 4070
2017	Special	Feb 6, 2017	2:00 pm – 2:30 pm	SMT 4240
(via FL2016-12)	Annual	Mar 27, 2017	12:00 pm – 1:00 pm	SMT 4070
	Regular	Jun 12, 2017	12:00 pm – 1:00 pm	SMT 4070
	Regular	Sep 25, 2017	12:00 pm – 1:00 pm	SMT 4070
	Regular	Dec 11, 2017	12:00 pm – 1:00 pm	SMT 4070
2016	Special	Jan 19, 2016	11:00 am – 12:00 pm	SMT 4080
(via FL2016-01)	Regular	Jan 25, 2016	12:00 pm – 1:00 pm	SMT 4070
	Annual	Mar 28, 2016	12:00 pm – 1:00 pm	SMT 4070
	Regular	May 23, 2016	12:00 pm – 1:00 pm	SMT 4070
	Special	Jun 3, 2016	12:00 pm – 1:00 pm	SMT 4090
	Special	Jun 27, 2016	10:00 am – 11:00 am	SMT 4070
	Regular	Sep 26, 2016	12:00 pm – 1:00 pm	SMT 4070
	Special	Nov 18, 2016	10:30 am – 11:00 am	SMT 4090
	Regular	Dec 12, 2016	12:00 pm – 1:00 pm	SMT 4070
2015	Special	Jan 26, 2015	12:00 pm – 1:00 pm	SMT 4070
(via FL2015-01)	Annual	Mar 23, 2015	12:00 pm – 1:00 pm	SMT 4070
	Regular	Apr 27, 2015	12:00 pm – 1:00 pm	SMT 4070
	Special	May 14, 2015	CANCELLED	
	Regular	May 26, 2015	11:30 am – 1:30 pm	SMT 4070
	Regular	Jul 27, 2015	12:00 pm – 1:00 pm	SMT 4070
	Regular	Sep 28, 2015	12:00 pm – 1:00 pm	SMT 4070

Executive Board Meeting Schedule

	Regular	Dec 14, 2015	12:00 pm – 1:00 pm	SMT 4070
2014	Annual	Mar 24, 2014	12:00 pm – 1:00 pm	SMT 4070
(via FL2014-03)	Regular	Apr 28, 2014	12:00 pm – 1:00 pm	SMT 4070
	Regular	May 27, 2014	9:00 am – 10:00 am	SMT 4070
	Regular	Jun 23, 2014	**CANCELLED**	
	Special	Jul 16, 2014	2:00 pm – 4:00 pm	SMT 4090
	Regular	Sep 22, 2014	12:00 pm – 1:00 pm	SMT 4070
	Regular	Dec 15, 2014	12:00 pm – 1:00 pm	SMT 4070

FileLocal

700 5th Avenue, Suite 4350
PO Box 94669
Seattle, WA 98124-4669

File Local Resolution FL2020-08
Briefing Paper Leviathan Security Group Contract

Date: September 30, 2020

Issue: Shall the Washington Multi-City Business License and Tax Portal Agency ("Agency") Executive Board authorize the Chair to execute a contract for Tax Portal Security Services with Leviathan?

Operating Committee Recommendation: The Portal Agency Executive Board should pass Resolution FL2020-08 approving the continued use of Leviathan as the Agency's Security Services vendor.

Rationale: Pursuant to Section 4 of the Washington Multi-City Business License and Tax Portal Agency Interlocal Agreement, guiding principals for Agency Security were established to ensure the integrity of the FileLocal product and City and Taxpayer Data. The Agency contracted with Leviathan during the implementation phase and after go-live of the originating/new cities. The Agency believes the vendor provides a unique service due to their history and familiarity with the existing system and key suppliers.

RESOLUTION NO. FL2020-08

A Resolution of the Washington Multi-City Business License and Tax Portal Agency Executive Board Authorizing a Contract with Leviathan Security Group for 2020-2022.

Whereas, Pursuant to Section 4 of the Washington Multi-City Business License and Tax Portal Agency Interlocal Agreement, guiding principles for Security were established to ensure the integrity of the FileLocal product and City and Taxpayer Data; and

Whereas, The City of Seattle contracted with Leviathan Security Group during the implementation phase and during the subsequent launch periods, and the Agency has since renewed its contractual relationship with Leviathan based on the quality, expertise, and timeliness of its services to the Agency; and

Whereas, the Agency would like to again retain Leviathan as its Security Vendor to ensure the product and data remain safe and secure for users and Participating Cities;

BE IT RESOLVED by the Executive Board of the Washington Multi-City Business License and Tax Portal Agency:

SECTION 1. The Executive Board authorizes the Chair to execute a contract with Leviathan Security Group as set forth in Attachment A to this Resolution.

ADOPTED this 30th day of September, 2020.

ATTEST:

Washington Multi-City Business License and Tax Portal Agency Executive Board
Seattle, Washington

Board Secretary

Board Chair

EXHIBIT A

SCOPE OF WORK

Consultant shall provide the following services:

1.1. Interim CISO: Company will provide temporary Interim Chief Information Security Officer (CISO) staff augmentation support on a retained basis in support of the Client Information Security Management Program. Shea Nangle, or other Company assigned staff pre-approved by Client, will act at Client written direction to complete duties as Client CISO of Record and/or trusted advisor SME guidance and strategic leadership support. Additional duties of Client CISO of Record shall, in conjunction with Client, manage Client's response to security audit questionnaires and other requests as required by Client's customers. Duties may include completing questionnaires and participating in conference calls with Client's customers. Additionally, Company will review services performed by Client's vendors and will review and advise upon the content of assessment reports provided by Client's vendors.

1.2. Refine Adopted Policies: Company will review existing information security policies and procedures. Following this process, Company will assist with the development and revision of relevant policies and procedures. Policies will be aligned with existing Client processes and procedures.

1.3. Vulnerability Assessment and Management Process: Company will provide ongoing support to ensure the smooth operation of the Vulnerability Assessment and Management process, assisting in prioritization, risk assessment and artifact generation / follow through on the part of the operations teams.

1.4. Security Incident Management: Company to provide Security Incident Management and Support as necessary to ensure that Client operations may be resumed as quickly as possible. Following any security incidents, Company will provide an after-action report that includes information such as documentation of the incident itself, the results of root cause analysis, and any and all actions taken to reduce the risk of the incident occurring again.

1.5. Security Assessment: Company will provide an assessment of the FileLocal platform. Consultant security assessment will use a combination of automated and manual assessment methodologies and solely focus on identifying vulnerabilities in Internet-accessible interfaces. The Company will also perform an automated vulnerability assessment of the underlying infrastructure to identify security flaws. Company will evaluate for security and privacy vulnerabilities including, but not limited to, those found in the OWASP Top 10. These vulnerability and weakness categories include:

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging & Monitoring

1.5.1. Post-remediation Evaluation Assessment: Subsequent to Client implementation of remediation activities related to any identified Critical or High ranked vulnerabilities, Company will perform targeted re-testing and confirm the effectiveness of remediation activities.

1.5.2. Assessment Deliverable: Upon completion of the testing, the Company will provide a written report containing the following:

- Executive summary, including a high-level summary of the analysis and findings and prioritized recommendations for remediation
- A brief description of assessment methodologies.
- A detailed discussion of analysis results, including relevant findings, risk levels, and recommended corrective action.
- Appendices with relevant raw data, output, and reports from the analysis tools used during the engagement.

1.6. Executive summary: Company will provide a report including a high-level summary of the work accomplished over the preceding year.

EXHIBIT B

Hourly Rates

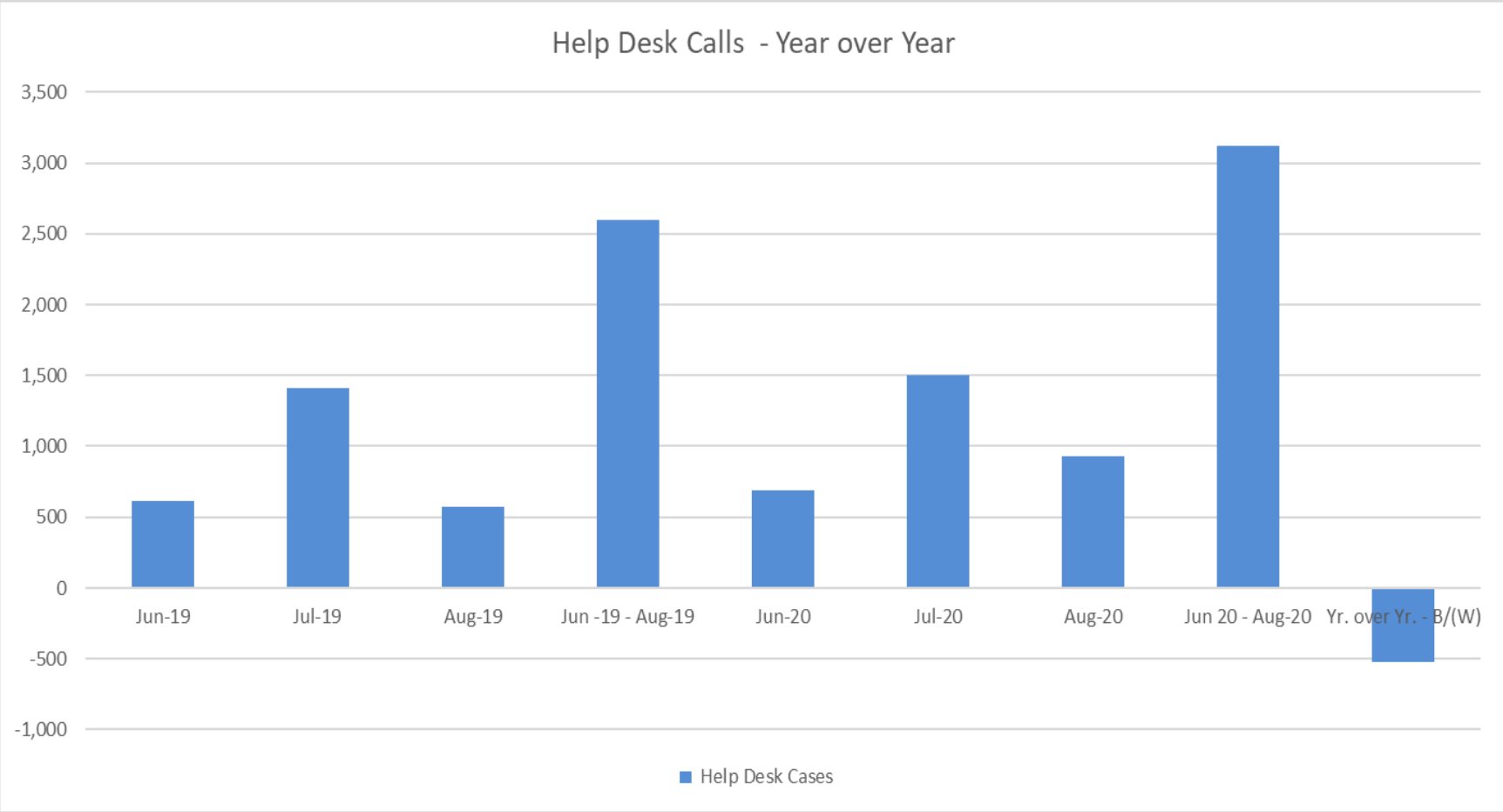
For all services provided as described in Exhibit A, the hourly rate of $300 shall apply.



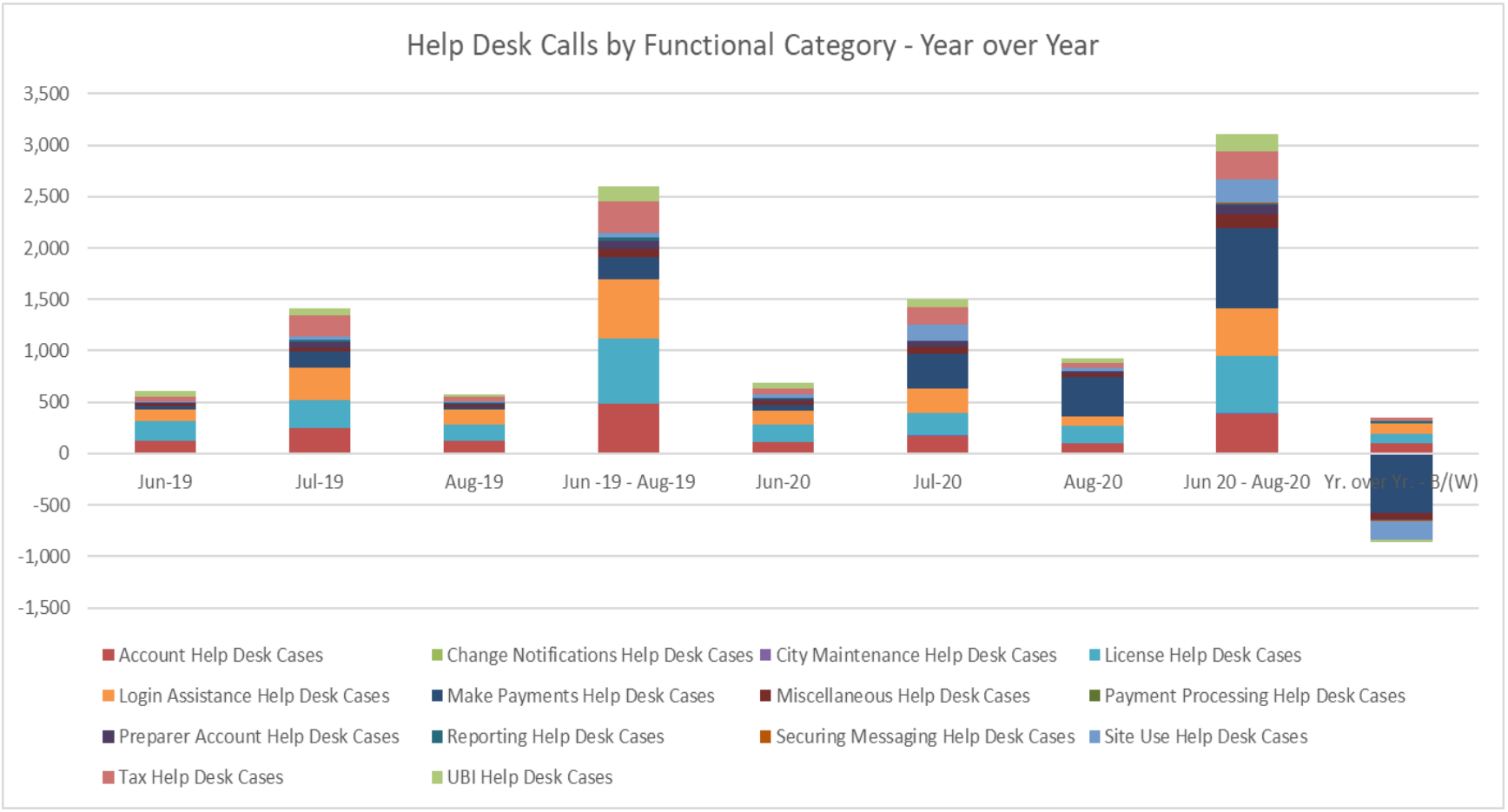
Help Desk Calls by Functional Category	Help desk calls totaled 3,121 for the three months ending August 2020. This is 10.3% of the accounts created and transactions processed which is .8% higher than the three months in the prior year. Payments are up significantly due to a payment processing issue in Kubra. The issue was resolved in early September.

FileLocal: Monthly Business Review

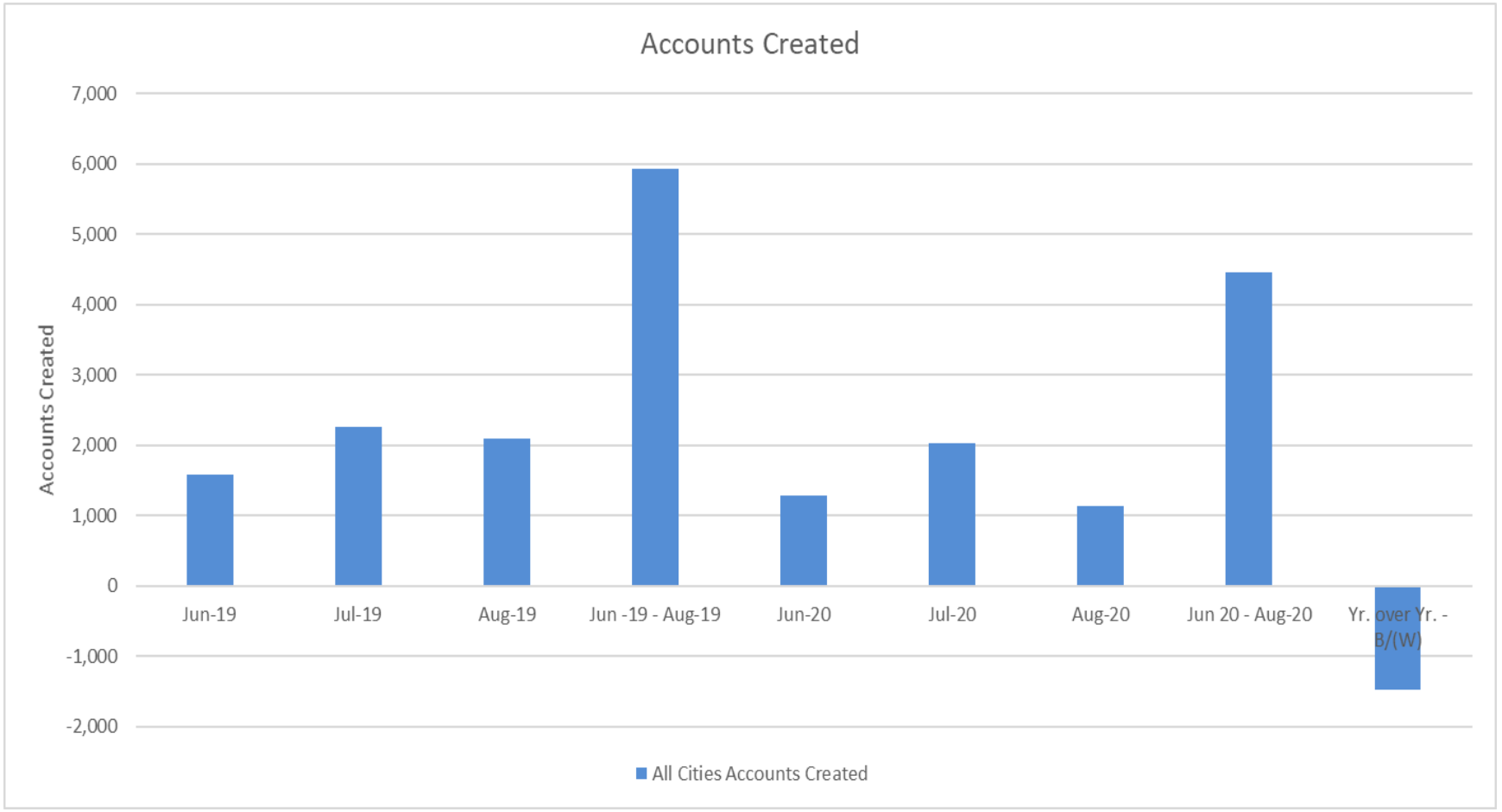
August 2020



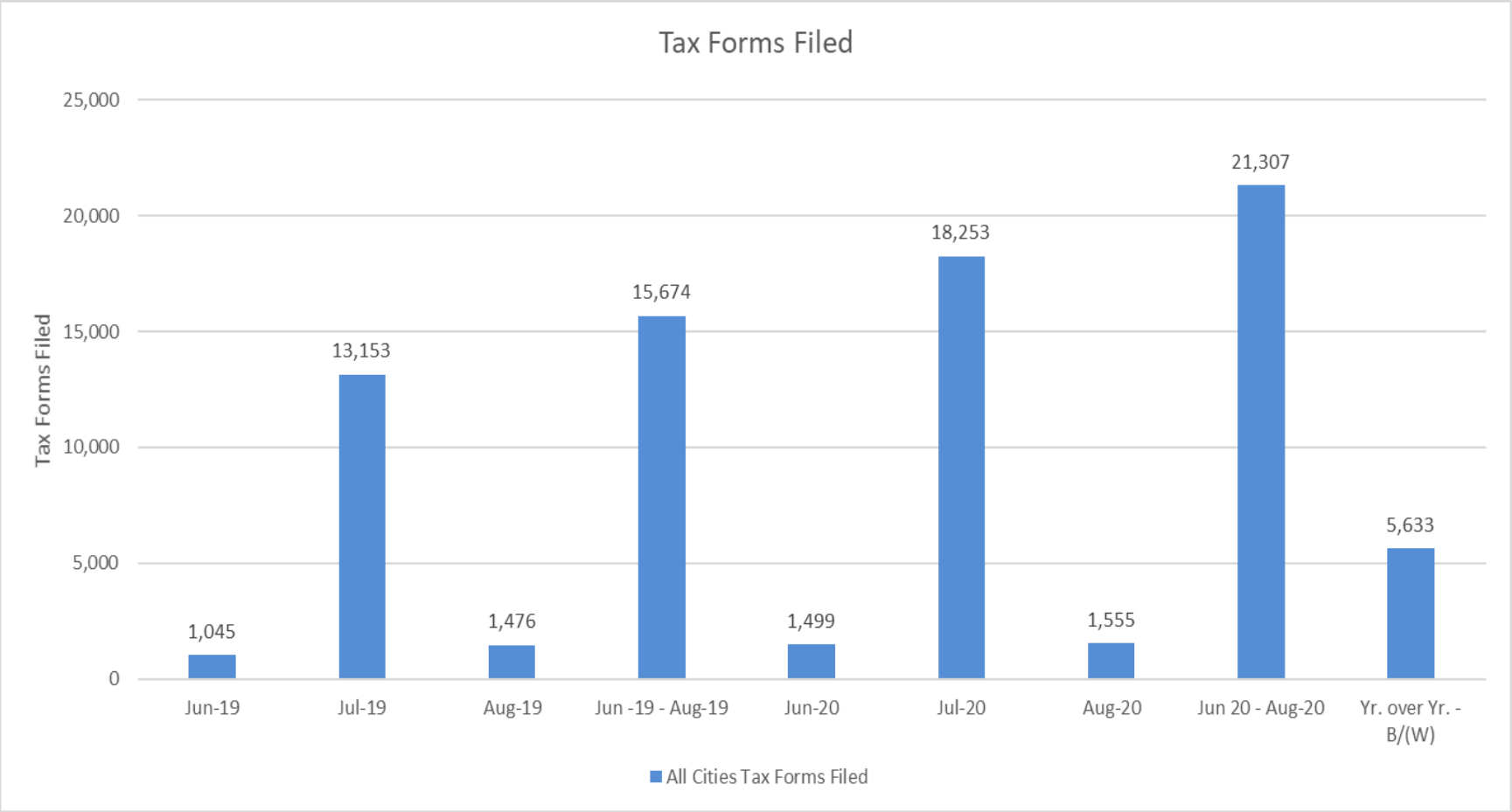
Help Desk Calls by Functional Category	Help desk calls totaled 3,121 for the three months ending August 2020. This is 10.5% of the accounts created and transactions processed which is .6% higher than the three months in the prior year. Payments are up significantly due to a payment processing issue in Kubra. The issue was reolved in early September.



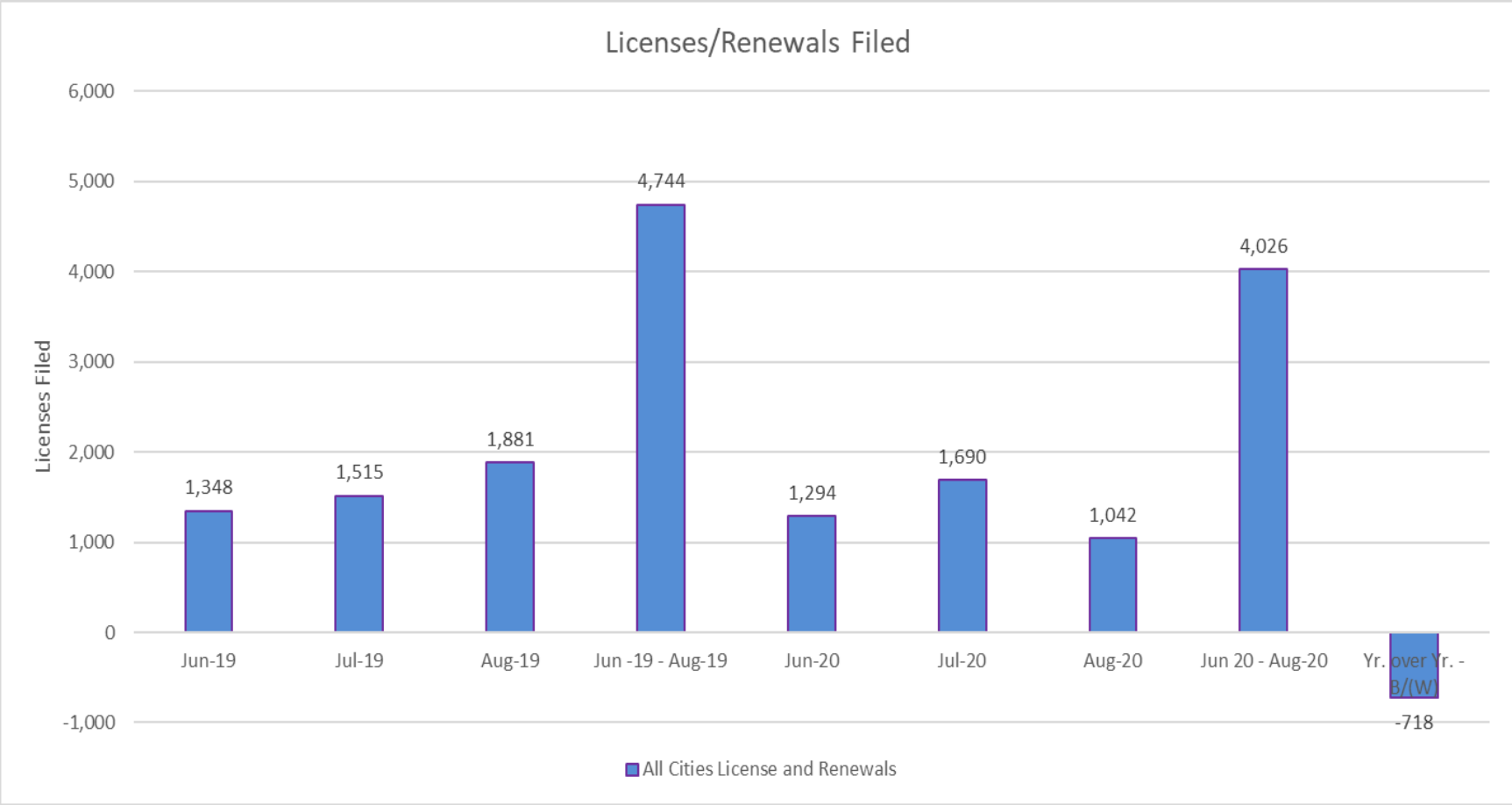
Help Desk Calls by Functional Category	Help desk calls totaled 3,121 for the three months ending August 2020. This is 10.5% of the accounts created and transactions processed which is .6% higher than the three months in the prior year. Payments are up significantly due to a payment processing issue in Kubra. The issue was reolved in early September.



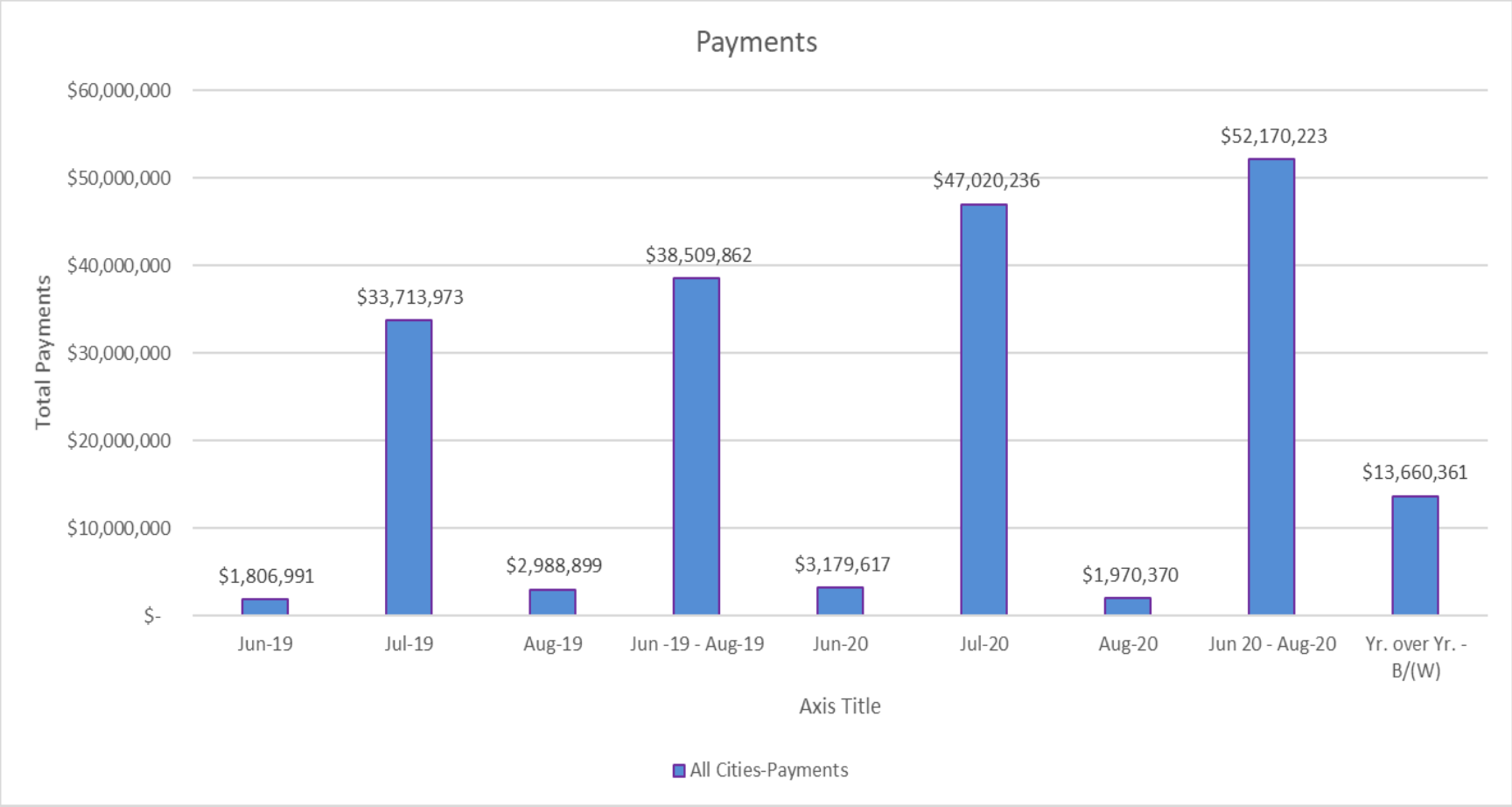
Accounts Created	Accounts created for the 3 months ended August 2020 were 4,456 which is down 1,475 accounts compared to the same 3 months in the prior year. 4 of the cities were up and 6 cities were down - Bellevue down 272, Bremerton up 7, Des Moines up 30, Everett down 329, Lake Forest Park down 4, Renton up 85, Seattle down 836, Shoreline down 26, Snoqualmie up 6 and Tacoma down 136.



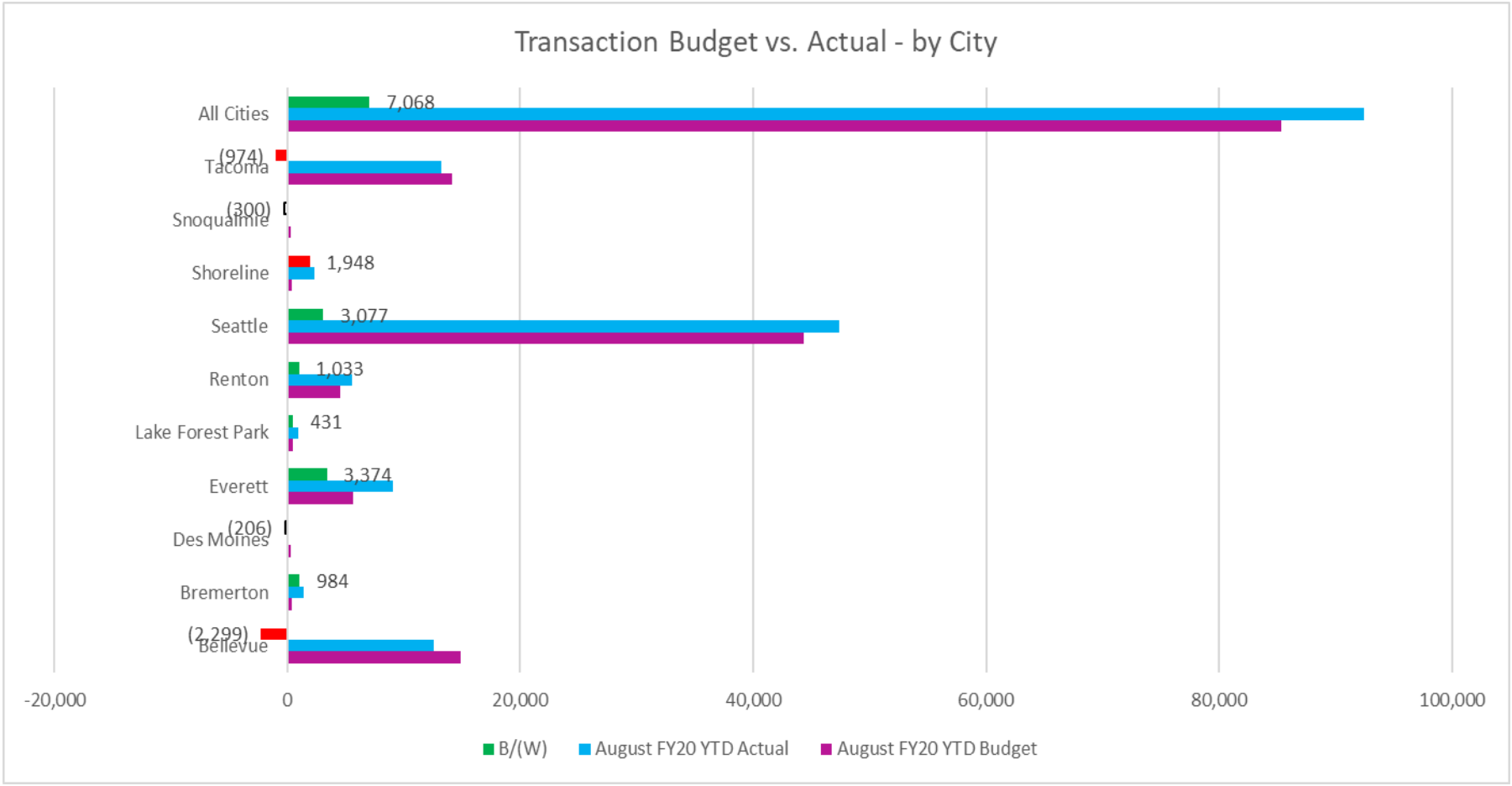
Tax Forms Filed	Tax Forms filed for the 3 months ended August 2020 were 21,307 which is up 5,633 filings compared to the same 3 months from the prior year. Nine cities were up and one city was down - Bellevue was down 515, Bremerton up 61, Des Moines up 30, Everett up 180, Lake Forest Park up 73, Renton up 629, Seattle up 4,821, Shoreline up 52, Snoqualmie up 6 and Tacoma up 296.



Licenses/Renewals Filed	License/Renewals created for the 3 months ended August 2020 were 4,026 which is down 718 filings compared to the same 3 months from the prior year. Seven cities were up and three cities were down - Bellevue up 29, Bremerton up 20, Des Moines up 86, Everett down 107, Lake Forest Park up 23, Renton up 199, Seattle down 1,158, Shoreline down 26, Snoqualmie up 16 and Tacoma up 200.



Payments Made by City	Payments made for the 3 months ended August 2020 were $52,170m which is up $13.7m compared to the same 3 months from the prior year. Eight of th cities were up and two cities were down with Bellevue down $492k Bremerton up $101k, Des Moines up 12.3k, Everett up $93k, Lake Forest Park up $18.2k, Renton down $527.2k, Seattle up $14,194k, Shoreline up $121k, Snoqualmie up .3 and Tacoma up $138.9k.



Transactions YTD Budget versus YTD Actual	Transactions YTD Budget versus Actual were favorable by 7,068. This is projects to 143.6k transactions for the year and $220m in payments.

User Account Sign-Up Metrics

Description	Jan-20	Feb-20	Mar-20	Apr-20	May-20	Jun-20	Jul-20	Aug-20
Users that completed email validation	5,544	1,766	1,395	3,165	1,242	1,155	1,680	1,015
% of users that completed email validation	95%	98%	98%	98%	97%	98%	97%	97%
Users that completed email validation and assigned a license	3,549	1,095	899	2,364	898	796	1,173	722
% of users that completed email validation and assigned a license	64%	62%	64%	75%	72%	69%	70%	71%
Filed a Tax Return for the First Time	1,793	602	459	1,522	485	430	662	332

Seattle Import Account Sign-Up Metrics

Description	Jan-20	Feb-20	Mar-20	Apr-20	May-20	Jun-20	Jul-20	Aug-20
Seattle Import Started	166	34	24	139	28	14	36	9
Seattle Import Completed	142	31	22	132	24	13	34	7
Seattle - % that started and completed import	86%	91%	92%	95%	86%	93%	94%	78%

January Postmortem

September 2020

Project Team

- Avenu Team was created to address the January Issues

System Performance Issues

- **Software**
  - Record Kubra File import ← **Testing phase**
  - Refactor Website Code (EF) ← **Analysis phase**
  - Logic to restrict deletion of data
  - Change the PCS logging
  - Batch Processor improve error logging
  - Batch Processor improve data fetching and updating
  - Add DB Referential Integrity
  - Enhance Relational DB Model
  - Add notification for batch summary report

System Performance Issues (continued)

- **Hardware**
  - Short Term (January 2020)
    - Added CPU, RAM and Hardware Storage
  - **Longer Term – Hardware Updated 9-16-20**
    - New Windows Server OS
    - Microsoft SQL
- **Measurement**
  - Baseline versus Improvement

- **Monitoring**
  - Daily Hardware Utilization Reports – Q2’20
    - RAM Utilization
    - Storage Utilization
    - CPU Utilization
  - **Software Error Log Monitoring – Q4’20**
  - **Help Desk Monitoring** – customized to reflect FileLocal specific metrics. ***In process Q3’20***.

- **Help Desk**
  - New Help Desk Software acquired and was planned for deployment 4-1-20 but delayed due to COVID-19. Agency to work with Avenu on the timing.
  - Help Desk Staffing
    - Staff is currently at 12 with an additional 30 staff members trained to answer calls
      - Codesmart – third party vendor to take overflow

- **Batch Issues**
  - December 2019 – July 2020 Recons/City Reviews In Process
    - Inputs
      - Remittance Files – 79k
      - Batch Reports – 104k
      - Rejection Reports – 1k
    - Outputs
      - Matched Items 79k
      - $0 Filings 25k
      - Reconciling Items .4k - City Meetings to Review

Agency Survey Action Items Update

September 2020

Agency Survey Action Items

- **Explore opportunities to extend HB 2005 (7/2020) deadline**
  - City of Kent ~Q1'21
- **Communicate city metrics beyond Board/OC members**
  - Tuesday meeting.
- **Work with vendors to distribute transaction level reports**
  - In progress – daily/monthly reports.
- **Identify ways to improve city/vendor portal integration**
  - ***Hardware, Software, Monitoring and Help Desk***
- **Explore options for allowing direct interactions between cities IT groups and vendors**
  - Pending system work by Avenu.
- **Work with subscriber cities to improve their experience**
  - Post portal integration work.
- **Modify survey to eliminate question confusion**
  - Created.
- **Work with Board to create a post July 2020 vision for the Agency**
  - Q4'20.

Americans With Disabilities Act (ADA) Audit Update

September 2020

September 2020

- FY2020 No ADA Updates – work to resume once the foundational software work is completed.

New Cities Update

September 2020

New City Status

Your one stop for local business licensing and tax filing

www.filelocal-wa.gov

City	Launch	Type	Notes
Des Moines	Launched Q2'2020	Principal	City has signed with FileLocal. City will convert to web service following implementation of a new SOR.
Snoqualmie	Launched Q2'2020	Subscriber	City has signed with FileLocal. City will convert to web service following implementation of a new SOR.
Kent	2021	Principal	City has notified the Agency that they would like to join FileLocal for Licensing only. City is building current SOR. Q1'21 estimated on boarding.

Vendor Warrants

September 2020

FileLocal
Quarterly Warrant List
June 30, 2020

Vendor Name	Payment for Current Quarter	Payments Year-To-Date
Association Recreational Council	-	10.00
Association of Washington Cities	300.00	300.00
City of Seattle Treasury Dept	97,330.38	206,919.40
City of Tacoma Tax & License	-	110.00
e.Gov Systems	283,845.50	304,403.00
Francis & Company	-	7,863.00
Keeney's	-	73.34
Kevin Fitzpatrick	-	586.70
Leviathan	5,312.50	9,250.00
Lund Consulting	-	4,562.50
Madrona Law Group, PLLC	1,530.00	8,730.00
Washington Cities Insurance Authority	-	5,164.00
Wendy Thomaston	31.08	31.08