FileLocal

Executive Board:

Toni Call
City of Bellevue

Susy Haugen
City of Everett

Chris Bothwell
City of Lake Forest Park

Jan Hawn
City of Renton

Glen Lee
City of Seattle

Andy Cherullo
City of Tacoma

Executive Board Agenda

March 28, 2019

SEATTLE MUNICIPAL TOWER CONFERENCE ROOM 4070
SEATTLE, WA

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

2. **PUBLIC COMMENT***

3. **APPROVAL OF 12-10-18 MEETING SUMMARY**
   a. 12-10-18 Meeting Summary

4. **REVIEW OF FEBRUARY, JANUARY 2019 AND DECEMBER 2018 FINANCIAL STATEMENTS**
   a. February 2019 Financial Statements
   b. January 2019 Financial Statements
   c. December 2018 Financial Statements
   d. November 2018 Financial Statements

5. **ACTION ITEMS**
   a. Resolution **FL2019-01: Francis & Company Accounting Services Contract Extension**
      i. Briefing Paper: **FL2019-01**
      ii. Resolution: **FL2019-01**
      iii. Attachment A: **FL2019-01**
   b. Resolution **FL2019-02**: **Kenyon Disend Legal Services Contract Extension**
      i. Briefing Paper: **FL2019-02**
      ii. Resolution: **FL2019-02**
      iii. Attachment A: **FL2019-02**
   c. Resolution **FL2019-03: IT Policy Manual Updates**
      i. Briefing Paper: **FL2019-03**
      ii. Resolution: **FL2019-03**
      iii. Attachment A: **FL2019-03**
      iv. Attachment B: **FL2019-03**
      v. Attachment C: **FL2019-03**

6. **OPERATIONAL UPDATES**
   a. Monthly Business Report

*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. OTHER BUSINESS

a. Budget
b. State Audit
c. ADA Update
d. Bremerton Update
e. New Cities Update
f. Vendor warrants

8. ADJOURNMENT

Your one stop for local business licensing and tax filing

www.filelocal.org

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

Executive Board:

Toni Call,
City of Bellevue

Susy Haugen,
City of Everett

Chris Bothwell, Chair,
City of Lake Forest Park

Jan Hawn
City of Renton

Glen Lee
City of Seattle

Andy Cherullo
City of Tacoma

Executive Board Meeting Summary

December 10, 2018

SEATTLE MUNICIPAL TOWER CONFERENCE ROOM 4070
SEATTLE, WA

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

Standing Items

1. CALL TO ORDER

The12-10-18, meeting of the Washington Multi-City Business License and Tax Portal Agency (FileLocal) was called to order at 12:06 p.m. and held in Conference Room 4070 of the Seattle Municipal Tower in Seattle, Washington.

ROLL CALL

Board Members Present: Toni Call (phone), Susy Haugen (phone), Aurora Belli (phone) for Chris Bothwell, Jan Hawn (phone), Glen Lee (phone), Andy Cherullo (phone).

Staff and Guests: David Linehan (phone), Horace Francis (phone), Kevin Fitzpatrick, and Julie Panick.

2. PUBLIC COMMENT

There were no public comments.

3. APPROVAL OF MEETING SUMMARY

On a motion made by Susy Haugen and seconded by Glen Lee, the board approved the 9-24-18, meeting summary.

4. REVIEW OF FINANCIAL STATEMENTS

Kevin Fitzpatrick summarized the October, September, and August financial statements and cash status. There were no questions or comments.

*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.

5. ACTION ITEMS

A. Resolution 2018-11 Meeting Schedule

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

i. Motion to accept: Andy Cherullo

ii. Motion seconded: Glen Lee

b. Majority Vote - passed

VOTE FL2018-11	**City**	**Member**
YES	Bellevue	Toni Call
YES	Everett	Susy Haugen
YES	Lake Forest Park	Aurora Belli
YES	Renton	Jan Hawn
YES	Seattle	Glen Lee
YES	Tacoma	Andy Cherullo

B. Resolution 2018-12 Final Budget

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

i. Supermajority vote discussion was led by Toni Call

ii. Motion to accept: Jan Hawn

iii. Motion seconded: Andy Cherullo

b. Supermajority Vote – passed

VOTE FL2018-12	**City**	**Member**
YES	Bellevue	Toni Call
YES	Everett	Susy Haugen
YES	Seattle	Glen Lee
YES	Tacoma	Andy Cherullo

c. Majority Vote - passed

VOTE FL2018-12	**City**	**Member**
YES	Bellevue	Toni Call
YES	Everett	Susy Haugen
YES	Lake Forest Park	Aurora Belli
YES	Renton	Jan Hawn
YES	Seattle	Glen Lee
YES	Tacoma	Andy Cherullo

6. DISCUSSION ITEMS:

A. August Monthly Business Review.

a. Help Desks calls are 2.6% lower than same 3-month period (Aug-Oct) in FY17.

b. Accounts created are up by 604 from FY17.

c. Tax forms filed shows significant growth for all cities.

d. License and Renewals shows significant growth for Bellevue, Everett, Renton, and Seattle.

B. New Cities Updates

a. Kevin reviewed the new cities status. There were no questions or comments.

C. Vendor Warrants

a. Reviewed the vendor warrants for Q4'18.

7. ADJOURNMENT:

On a motion made by Jan Hawn and seconded by Susy Haugen, the meeting of the Executive Board adjourned at 12:36 p.m.

Respectfully Submitted,

Julie Panick
Secretary, FileLocal

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

FileLocal
Financial Statements
February 28, 2019

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
FEBURARY 28, 2019

ASSETS		
Cash	**$**	**704,453**
Accounts receivable		**681,854**
Dues from Cities		**17,237**
Prepaid		**4,615**
Total Current Assets		**1,408,159**
TOTAL ASSETS	**$**	**1,408,159**
LIABILITIES AND NET ASSETS		
LIABILITIES		
Accounts payable	**$**	**165,045**
Accrued liabilities		**104,597**
Total Current Liabilities		**269,642**
TOTAL LIABILITIES	**$**	**269,642**
NET ASSETS		
Net assets, unrestricted	**$**	**450,921**
Change in net assets		**687,596**
TOTAL NET ASSETS	**$**	**1,138,517**
TOTAL LIABILITIES AND NET ASSETS	**$**	**1,408,159**

FILELOCAL
STATEMENT OF ACTIVITIES
FOR THE THREE MONTHS
AND YEAR-TO-DATE ENDED FEBURARY 28, 2019

	January	Feburary		YTD
REVENUES				
User fees	67,964	13,856	**$**	**81,820**
Reimbursable cost/Capital cost recovery charges				
City of Seattle	483,703	-		**483,703**
City of Bellevue	76,517	-		**76,517**
City of Tacoma	119,827	-		**119,827**
City of Everett	34,760	-		**34,760**
City of Lake Forest Park	8,932	-		**8,932**
City of Bremerton	-	-		**-**
City of Renton	36,060	-		**36,060**
City of Shoreline	14,326	-		**14,326**
Total direct reimbursable costs	774,125	-		**774,125**
Shared cost reimbursements	-	-		**-**
Total revenues	842,089	13,856	**$**	**855,945**
EXPENSES				
Accounting fees	2,595	3,351	**$**	**5,946**
Agency IT costs	-	-		**-**
Bank fees	-	-		**-**
Capital Recovery Payment	-	-		**-**
Conference cost	-	-		**-**
Consulting	-	-		**-**
Insurance	433	433		**866**
Labor costs	33,188	25,394		**58,582**
Legal fees	300	-		**300**
License and membership fees	420	-		**420**
Meals and entertainment	-	-		**-**
Office and operation supplies	-	-		**-**
Printing and copying	-	-		**-**
Technology costs	26,350	25,950		**52,300**
Transaction fees	25,487	24,448		**49,935**
Travel Expense	-	-		**-**
Reimbursable Shared Costs	-	-		**-**
Total expenses	88,772	79,575	**$**	**168,349**
CHANGE IN NET ASSETS	753,317	(65,719)	**$**	**687,596**

FILELOCAL
SCHEDULE OF BUDGET AND ACTUAL
FOR THE YEAR TO DATE ENDED FEBURARY 28, 2019

	Budget	YTD Budget	YTD Actual	Variance
REVENUES				
User fees	$ 328,001	$ 54,667	$ 81,820	$ 27,153
Reimbursable cost/Capital cost recovery charges				
City of Seattle	483,703	483,703	483,703	-
City of Bellevue	76,517	76,517	76,517	-
City of Tacoma	119,827	119,827	119,827	-
City of Everett	34,760	34,760	34,760	-
City of Lake Forest Park	8,932	8,932	8,932	-
City of Bremerton	37,091	37,091	-	(37,091)
City of Renton	36,060	36,060	36,060	-
City of Shoreline	14,326	14,326	14,326	-
Total direct reimbursable costs	811,216	811,216	774,125	(37,091)
Other				
Fund carryover	50,000	$ 50,000	$ -	$ (50,000)
Total sources	$ 1,189,217	$ 915,883	$ 855,945	$ (59,938)
EXPENSES				
Labor costs	$ 398,257	$ 66,376	$ 58,582	$ 7,794
Contracts	$ 59,788	9,965	6,812	3,153
Overhead	$ 54,396	9,066	720	8,346
Technology costs	631,683	105,281	102,235	3,046
Operating reserve	27,094	4,516	-	4,516
Capital cost recovery payments	18,000	3,000	-	3,000
Consulting	-	-	-	-
Meals and entertainment	-	-	-	-
Total operating expenses	$ 1,189,218	$ 198,204	$ 168,349	$ 29,855
CHANGE IN NET ASSETS			687,596	
NET ASSETS, AS OF JANUARY 1, 2019			450,921	
NET ASSETS, AS OF FEBRUARY 28, 2019			$ 1,138,517	
Schedule I - Contracts				
Accounting	$ 40,880	$ 6,813	$ 5,946	$ 867
Auditing	11,202	1,867	-	1,867
Insurance	6,162	1,027	866	161
Bank fees	1,544	257	-	257
Total	$ 59,788	$ 9,965	$ 6,812	$ 3,153
Schedule II - Overhead				
Legal	$ 33,366	$ 5,561	$ 300	$ 5,261
Office and operating supplies	3,503	584	-	584
Printing	3,503	584	-	584
Licenses/Memberships	3,503	584	420	164
Agency IT costs	3,762	627	-	627
Marketing	6,759	1,127	-	1,127
Total	$ 54,396	$ 9,066	$ 720	$ 8,346

FILELOCAL
STATEMENT OF CASHFLOW
FOR THE YEAR TO DATE ENDED FEBURARY 28, 2019

		FEBURARY 28
Change in Net Assets	$	687,596
Adjustments to reconcile Change in Net Assets		
to net cash provided by operations:		
Accounts Receivable		(635,148)
Dues from Cities		-
Prepaid		(3,995)
Accounts Payable and Accrued Liabilities		68,979
Net cash increase for two months ending 2/28/2019		117,432
Cash at 1/1/2019		587,022
Cash at 2/28/2019		**704,453**
Less Operating Reserve		**172,985**
Cash Available	**$**	**531,468**

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

FileLocal
Financial Statements
January 31, 2019

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
JANUARY 31, 2019

ASSETS		
Cash	**$**	**561,795**
Accounts receivable		**823,011**
Dues from Cities		**17,237**
Prepaid		**5,048**
Total Current Assets		**1,407,091**
TOTAL ASSETS	**$**	**1,407,091**
LIABILITIES AND NET ASSETS		
LIABILITIES		
Accounts payable	**$**	**119,679**
Accrued liabilities		**83,175**
Total Current Liabilities		**202,854**
TOTAL LIABILITIES	**$**	**202,854**
NET ASSETS		
Net assets, unrestricted	**$**	**450,921**
Change in net assets		**753,316**
TOTAL NET ASSETS	**$**	**1,204,237**
TOTAL LIABILITIES AND NET ASSETS	**$**	**1,407,091**

FILELOCAL
STATEMENT OF ACTIVITIES
FOR THE THREE MONTHS
AND YEAR-TO-DATE ENDED JANUARY 31, 2019

	January	YTD
REVENUES		
User fees	67,964	**$ 67,964**
Reimbursable cost/Capital cost recovery charges		
City of Seattle	483,703	**483,703**
City of Bellevue	76,517	**76,517**
City of Tacoma	119,827	**119,827**
City of Everett	34,760	**34,760**
City of Lake Forest Park	8,932	**8,932**
City of Bremerton	-	**-**
City of Renton	36,060	**36,060**
City of Shoreline	14,326	**14,326**
Total direct reimbursable costs	774,125	**774,125**
Shared cost reimbursements	-	**-**
Total revenues	842,089	**$ 842,089**
EXPENSES		
Accounting fees	2,595	**$ 2,595**
Agency IT costs	-	**-**
Bank fees	-	**-**
Capital Recovery Payment	-	**-**
Conference cost	-	**-**
Consulting	-	**-**
Insurance	433	**433**
Labor costs	33,188	**33,188**
Legal fees	300	**300**
License and membership fees	420	**420**
Meals and entertainment	-	**-**
Office and operation supplies	-	**-**
Printing and copying	-	**-**
Technology costs	26,350	**26,350**
Transaction fees	25,487	**25,487**
Travel Expense	-	**-**
Reimbursable Shared Costs	-	**-**
Total expenses	88,772	**$ 88,773**
CHANGE IN NET ASSETS	753,317	**$ 753,316**

FILELOCAL
SCHEDULE OF BUDGET AND ACTUAL
FOR THE YEAR TO DATE ENDED JANUARY 31, 2019

	Budget	YTD Budget	YTD Actual	Variance
REVENUES				
User fees	$ 328,001	$ 27,333	$ 67,964	$ 40,631
Reimbursable cost/Capital cost recovery charges				
City of Seattle	483,703	483,703	483,703	-
City of Bellevue	76,517	76,517	76,517	-
City of Tacoma	119,827	119,827	119,827	-
City of Everett	34,760	34,760	34,760	-
City of Lake Forest Park	8,932	8,932	8,932	-
City of Bremerton	37,091	37,091	-	(37,091)
City of Renton	36,060	36,060	36,060	-
City of Shoreline	14,326	14,326	14,326	-
Total direct reimbursable costs	811,216	811,216	774,125	(37,091)
Other				
Fund carryover	50,000	$ 50,000	$ -	$ (50,000)
Total sources	$ 1,189,217	$ 888,549	$ 842,089	$ (46,460)
EXPENSES				
Labor costs	$ 398,257	$ 33,188	$ 33,188	$ -
Contracts	$ 59,788	4,982	3,028	1,954
Overhead	$ 54,396	4,533	720	3,813
Technology costs	631,683	52,640	51,837	803
Operating reserve	27,094	2,258	-	2,258
Capital cost recovery payments	18,000	1,500	-	1,500
Consulting	-	-	-	-
Meals and entertainment	-	-	-	-
Total operating expenses	$ 1,189,218	$ 99,101	$ 88,773	$ 10,328
CHANGE IN NET ASSETS			753,316	
NET ASSETS, AS OF JANUARY 1, 2019			450,921	
NET ASSETS, AS OF JANUARY 31, 2019			$ 1,204,237	
Schedule I - Contracts				
Accounting	$ 40,880	$ 3,407	$ 2,595	$ 812
Auditing	11,202	934	-	934
Insurance	6,162	514	433	81
Bank fees	1,544	129	-	129
Total	$ 59,788	$ 4,984	$ 3,028	$ 1,954
Schedule II - Overhead				
Legal	$ 33,366	$ 2,781	$ 300	$ 2,481
Office and operating supplies	3,503	292	-	292
Printing	3,503	292	-	292
Licenses/Memberships	3,503	292	420	(128)
Agency IT costs	3,762	314	-	314
Marketing	6,759	563	-	563
Total	$ 54,396	$ 4,533	$ 720	$ 3,813

FILELOCAL
STATEMENT OF CASHFLOW
FOR THE YEAR TO DATE ENDED JANUARY 31, 2019

		JANUARY 31
Change in Net Assets	$	753,316
Adjustments to reconcile Change in Net Assets		
to net cash provided by operations:		
Accounts Receivable		(776,305)
Dues from Cities		-
Prepaid		(4,428)
Accounts Payable and Accrued Liabilities		2,191
Net cash increase for one months ending 1/31/2019		(25,226)
Cash at 1/1/2019		587,022
Cash at 1/31/2019		**561,795**
Less Operating Reserve		**172,985**
Cash Available	**$**	**388,810**

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

FileLocal
Financial Statements
December 31, 2018

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
DECEMBER 31, 2018

ASSETS		
Cash	**$**	**587,022**
Accounts receivable		**46,706**
Billable to Cities		**17,237**
Prepaid		**620**
Total Current Assets		**651,584**
TOTAL ASSETS	**$**	**651,584**
LIABILITIES AND NET ASSETS		
LIABILITIES		
Accounts payable	**$**	**193,163**
Accrued liabilities		**7,500**
Total Current Liabilities		**200,663**
TOTAL LIABILITIES	**$**	**200,663**
NET ASSETS		
Net assets, unrestricted	**$**	**395,500**
Net Income		**55,421**
TOTAL NET ASSETS	**$**	**450,921**
TOTAL LIABILITIES AND NET ASSETS	**$**	**651,584**

FILELOCAL
STATEMENT OF ACTIVITIES
FOR THE THREE MONTHS
AND YEAR-TO-DATE ENDED DECEMBER 31, 2018

	October	November	December	YTD
REVENUES				
User fees	$ 35,492	$ 20,904	27,064	**$ 212,329**
Reimbursable cost/Capital cost recovery charges				
City of Seattle	-	-	-	**543,559**
City of Bellevue	-	-	-	**85,125**
City of Tacoma	-	-	-	**133,922**
City of Everett	-	-	-	**38,821**
City of Lake Forest Park	-	-	-	**10,955**
City of Bremerton	-	-	-	**13,854**
City of Renton	-	-	-	**21,117**
City of Shoreline	-	-	6,465	**6,465**
Total direct reimbursable costs	-	-	6,465	**853,818**
Shared cost reimbursements	-	-	-	**-**
Total revenues	$ 35,492	$ 20,904	33,529	**$ 1,066,147**
EXPENSES				
Accounting fees	$ 2,500	$ (2,346)	2,833	**$ 36,763**
Agency IT costs	-	-	-	**-**
Bank fees	-	147	-	**147**
Capital Recovery Payment	-	-	21,000	**21,000**
Conference cost	-	-	-	**3,175**
Consulting	-	-	-	**-**
Insurance	433	433	425	**5,188**
Labor costs	74,711	27,483	47,278	**353,961**
Legal fees	-	568	1,000	**12,170**
License and membership fees	-	-	300	**635**
Meals and entertainment	-	-	131	**315**
Office and operation supplies	-	-	-	**151**
Printing and copying	-	-	-	**-**
Technology costs	70,071	15,400	47,075	**480,057**
Transaction fees	12,422	10,893	10,848	**94,340**
Travel Expense	611	-	135	**2,823**
Reimbursable Shared Costs	-	-	-	**-**
Total expenses	$ 160,748	$ 52,578	131,024	**$ 1,010,726**
CHANGE IN NET ASSETS	$ (125,256)	$ (31,674)	(97,495)	**$ 55,421**

FILELOCAL
SCHEDULE OF BUDGET AND ACTUAL
FOR THE YEAR TO DATE ENDED DECEMBER 31, 2018

	Budget	YTD Budget	YTD Actual	Variance
REVENUES				
User fees	$ 251,000	$ 251,000	$ 212,329	$ (38,671)
Reimbursable cost/Capital cost recovery charges				
City of Seattle	539,415	539,415	543,559	4,144
City of Bellevue	84,522	84,522	85,125	603
City of Tacoma	132,947	132,947	133,922	975
City of Everett	38,540	38,540	38,821	281
City of Lake Forest Park	10,886	10,886	10,955	69
City of Bremerton	19,118	19,118	13,854	(5,264)
City of Renton	19,623	19,623	21,117	1,494
City of Shoreline	4,465	4,465	6,465	2,000
Total direct reimbursable costs	849,516	849,516	853,818	4,302
Other				
Fund carryover	30,000			
Total sources	$ 1,130,516	$ 1,100,516	$ 1,066,147	$ (34,369)
EXPENSES				
Labor costs	$ 366,994	$ 366,994	$ 353,961	$ 13,033
Contracts	$ 45,670	45,670	42,098	3,572
Overhead	$ 60,183	60,183	18,954	41,229
Technology costs	573,993	573,993	574,397	(404)
Operating reserve	23,063	23,063	-	23,063
Capital cost recovery payments	21,000	21,000	21,000	0
Consulting	-	-	-	-
Meals and entertainment	-	-	315	315
Total operating expenses	$ 1,090,903	$ 1,090,903	$ 1,010,725	$ 80,178
CHANGE IN NET ASSETS			55,421	
NET ASSETS, AS OF JANUARY 1, 2018			395,500	
NET ASSETS, AS OF DECEMBER 31, 2018			$ 450,921	
Schedule I - Contracts				
Accounting	$ 27,169	$ 27,169	$ 36,763	$ (9,594)
Auditing	10,961	10,961	-	10,961
Insurance	6,029	6,029	5,188	841
Bank fees	1,511	1,511	147	1,364
Total	$ 45,670	$ 45,670	$ 42,098	$ 3,572
Schedule II - Overhead				
Legal	$ 32,648	$ 32,648	$ 12,170	$ 20,478
Office and operating supplies	6,236	6,236	151	6,085
Printing	6,236	6,236	-	6,236
Licenses/Memberships	6,236	6,236	3,458	2,778
Agency IT costs	2,947	2,947	-	2,947
Marketing	5,880	5,880	3,175	2,705
Total	$ 60,183	$ 60,183	$ 18,954	$ 41,229

FILELOCAL
STATEMENT OF CASHFLOW
FOR THE YEAR TO DATE ENDED DECEMBER 31, 2018

		DECEMBER 2018
Net Income		$ 55,421
Adjustments to reconcile Net Income		
to net cash provided by operations:		
	Accounts Receivable	(32,634)
	Billable to Cities	(22,502)
	Prepaid	310
	Accounts Payable and Accrued Liabilities	71,853
Net cash increase for twelve months ending 12/31/2018		72,448
Cash at 1/1/2018		514,574
Cash at 12/31/2018		**587,022**
Less Operating Reserve		**157,026**
Cash Available		**$ 429,996**

FileLocal

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

FileLocal
Financial Statements
November 30, 2018

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

FILELOCAL
STATEMENT OF FINANCIAL POSITION
NOVEMBER 30, 2018

ASSETS		
Cash	$	546,450
Accounts receivable		30,537
Billable to Cities		28,392
Prepaid		15,545
Total Current Assets		620,924
TOTAL ASSETS	$	620,924
LIABILITIES AND NET ASSETS		
LIABILITIES		
Accounts payable	$	7,461
Accrued liabilities		65,046
Total Current Liabilities		72,507
TOTAL LIABILITIES	$	72,507
NET ASSETS		
Net assets, unrestricted	$	395,500
Net Income		152,917
TOTAL NET ASSETS	$	548,417
TOTAL LIABILITIES AND NET ASSETS	$	620,924

FILELOCAL
STATEMENT OF ACTIVITIES
FOR THE THREE MONTHS
AND YEAR-TO-DATE ENDED NOVEMBER 30, 2018

	September	October	November	YTD
REVENUES				
User fees	$ 4,520	$ 35,492	$ 20,904	**$ 185,265**
Reimbursable cost/Capital cost recovery charges				
City of Seattle	-	-	-	**543,559**
City of Bellevue	-	-	-	**85,125**
City of Tacoma	-	-	-	**133,922**
City of Everett	-	-	-	**38,821**
City of Lake Forest Park	-	-	-	**10,955**
City of Bremerton	-	-	-	**13,854**
City of Renton	21,117	-	-	**21,117**
Total direct reimbursable costs	21,117	-	-	**847,353**
Shared cost reimbursements	-	-	-	**-**
Total revenues	$ 25,637	$ 35,492	$ 20,904	**$ 1,032,618**
EXPENSES				
Accounting fees	$ 2,500	$ 2,500	$ (2,346)	**$ 33,931**
Agency IT costs	-	-	-	**-**
Bank fees	-	-	147	**147**
Capital Recovery Payment	-	-	-	**-**
Conference cost	-	-	-	**3,175**
Consulting	-	-	-	**-**
Insurance	433	433	433	**4,763**
Labor costs	30,000	74,711	27,483	**306,683**
Legal fees	1,856.00	-	568	**11,170**
License and membership fees	-	-	-	**335**
Meals and entertainment	184.64	-	-	**185**
Office and operation supplies	5	-	-	**151**
Printing and copying	-	-	-	**-**
Technology costs	34,792	70,071	15,400	**432,983**
Transaction fees	2,912	12,422	10,893	**83,492**
Travel Expense	767	611	-	**2,688**
Reimbursable Shared Costs	-	-	-	**-**
Total expenses	$ 73,450	$ 160,748	$ 52,578	**$ 879,701**
CHANGE IN NET ASSETS	$ (47,813)	$ (125,256)	$ (31,674)	**$ 152,917**

FILELOCAL
SCHEDULE OF BUDGET AND ACTUAL
FOR THE YEAR TO DATE ENDED NOVEMBER 30, 2018

	Budget	YTD Budget	YTD Actual	Variance
REVENUES				
User fees	$ 251,000	$ 230,083	$ 185,265	$ (44,818)
Reimbursable cost/Capital cost recovery charges				
City of Seattle	539,415	539,415	543,559	4,144
City of Bellevue	84,522	84,522	85,125	603
City of Tacoma	132,947	132,947	133,922	975
City of Everett	38,540	38,540	38,821	281
City of Lake Forest Park	10,886	10,886	10,955	69
City of Bremerton	19,118	19,118	13,854	(5,264)
City of Renton	19,623	19,623	21,117	1,494
City of Shoreline	4,465	4,465	-	(4,465)
Total direct reimbursable costs	849,516	849,516	847,353	(2,163)
Other				
Fund carryover	30,000			
Total sources	$ 1,130,516	$ 1,079,599	$ 1,032,618	$ (46,981)
EXPENSES				
Labor costs	$ 366,994	$ 336,411	$ 306,683	$ 29,728
Contracts	$ 45,670	41,864	38,841	3,023
Overhead	$ 60,183	55,168	17,519	37,649
Technology costs	573,993	526,160	516,475	9,685
Operating reserve	23,063	21,141	-	21,141
Capital cost recovery payments	21,000	19,250	-	19,250
Consulting	-	-	-	-
Meals and entertainment	-	-	185	185
Total operating expenses	$ 1,090,903	$ 999,994	$ 879,701	$ 120,293
CHANGE IN NET ASSETS			152,917	
NET ASSETS, AS OF JANUARY 1, 2018			395,500	
NET ASSETS, AS OF NOVEMBER 30, 2018			$ 548,417	
Schedule I - Contracts				
Accounting	$ 27,169	$ 24,905	$ 33,931	$ (9,026)
Auditing	10,961	10,048	-	10,048
Insurance	6,029	5,526	4,763	763
Bank fees	1,511	1,385	147	1,238
Total	$ 45,670	$ 41,864	$ 38,841	$ 3,023
Schedule II - Overhead				
Legal	$ 32,648	$ 29,928	$ 11,170	$ 18,758
Office and operating supplies	6,236	5,716	151	5,565
Printing	6,236	5,716	-	5,716
Licenses/Memberships	6,236	5,716	3,023	2,693
Agency IT costs	2,947	2,701	-	2,701
Marketing	5,880	5,391	3,175	2,216
Total	$ 60,183	$ 55,168	$ 17,519	$ 37,649

FILELOCAL
STATEMENT OF CASHFLOW
FOR THE YEAR TO DATE ENDED NOVEMBER 30, 2018

		NOVEMBER 2018
Net Income		$ 152,917
Adjustments to reconcile Net Income		
to net cash provided by operations:		
	Accounts Receivable	(16,465)
	Billable to Cities	(33,657)
	Prepaid	(14,615)
	Accounts Payable and Accrued Liabilities	(56,303)
Net cash increase for eleven months ending 11/30/2018		31,876
Cash at 1/1/2018		514,574
Cash at 11/30/2018		**546,450**
Less Operating Reserve		**157,026**
Cash Available		**$ 389,424**

FileLocal

File Local Resolution FL2019-01
Briefing Paper Francis and Company Accounting Contract

Date: March 28, 2019

Issue: Shall the Washington Multi-City Business License and Tax Portal Agency ("Agency") Executive Board authorize the Program Manager to execute a contract for accounting services with Francis and Company for the years 2019-2020?

Operating Committee Recommendation: The Portal Agency Executive Board should pass Resolution FL2019-01 approving the continued use of Francis and Company as the Agency's accounting services vendor.

Rationale: Pursuant to Section 4 of the Washington Multi-City Business License and Tax Portal Agency Interlocal Agreement, guiding principles for Agency integrity and accountability were established for the Agency. The Executive Board is also empowered under Section 6 of the ILA to enter into contracts with third-parties for services necessary to fulfill the purposes of the Agency and Interlocal Agreement. The Agency contracted with Francis and Company as our initial accounting firm. The Agency believes the vendor provides a unique service due to their history and familiarity with the Agency.

RESOLUTION NO. FL2019-01

A Resolution of the Washington Multi-City Business License and Tax Portal Agency Executive Board Authorizing a Contract with Francis and Company to Provide Accounting Services for 2019-2020.

Whereas, Pursuant to Section 4 of the Washington Multi-City Business License and Tax Portal Agency Interlocal Agreement, guiding principles of integrity and accountability were established for the FileLocal Agency; and

Whereas, Pursuant to Section 6 of the Washington Multi-City Business License and Tax Portal Agency Interlocal Agreement, the Executive Board of the FileLocal Agency has the power to enter into agreements with third parties for the provision of services necessary to fully implement the purposes of the Agency and the Interlocal Agreement; and

Whereas, The City of Seattle contracted with Francis and Company to provide accounting services during the implementation phase and during the subsequent launch period, and the Agency would like to retain Francis and Company as its accounting vendor due to its history and familiarity with the Agency;

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 Program Manager to execute a contract with Francis and Company substantially in the form as set forth in Attachment A to this Resolution.

ADOPTED this 28th day of March, 2019.

ATTEST:

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

Board Secretary

Board Chair

CONSULTANT SERVICES CONTRACT BETWEEN THE WASHINGTON MULTI-CITY BUSINESS LICENSE AND TAX PORTAL AGENCY AND FRANCIS & COMPANY, PLLC, FOR ACCOUNTING AND TREASURER SERVICES

This Agreement ("Agreement") is made by and between the Washington Multi-City Business License and Tax Portal Agency d/b/a FileLocal ("Agency"), and Francis & Company, PLLC (hereinafter the "Consultant"), a corporation organized under the laws of the State of Washington, located and doing business at 200 W. Mercer St., Suite 208, Seattle, WA 98119.

RECITALS

WHEREAS, the Agency is required by law and its Fiscal Manual to prepare annual budgets, maintain accurate accounting and financial records, and implement financial controls; and

WHEREAS, the Agency previously selected Consultant to provide accounting and financial management services, and Consultant has provided such services pursuant to previously executed contracts; and

WHEREAS, the Agency recognizes Consultant's expertise and extensive knowledge of Agency's financial policies, procedures, and operations in this area and desires for Consultant to continue providing Agency with such services, and Consultant has agreed to provide these services on the terms and conditions provided in this Agreement;

NOW, THEREFORE, in consideration of the mutual promises set forth herein, it is agreed by and between the parties as follows:

TERMS

I. Description of Work.

Consultant shall perform the services specified in Exhibit A ("Scope of Services") attached hereto. Consultant represents and warrants that it and any staff member assigned to the work will have the requisite training, skill, and experience necessary to provide the services required by this Agreement and, where required, is/are appropriately accredited and licensed by all applicable agencies and governmental entities. Services provided by Consultant and its subconsultant(s) under this Agreement will be performed in a manner consistent with that degree of care and skill ordinarily exercised by members of the same profession currently practicing in similar circumstances. Consultant shall not subcontract for the performance of any work under this Agreement without prior written permission of the Agency.

II. Payment

A. The Agency shall pay Consultant an amount based on Consultant's hourly rates for the services described in Section I herein. The total compensation to be paid to Consultant for services provided under this Agreement shall not exceed $35,000 in any calendar year except upon approval in advance and in writing by the Agency. Consultant shall bill Agency based on the hourly rates and charges attached hereto as Exhibit B ("Consultant's Hourly Rates and Charges") and incorporated herein by this reference.

B. Consultant shall submit monthly invoices to the Agency for all work performed during the previous month. The Agency shall pay the full amount of an invoice within sixty (60) days of receipt. If the Agency objects to all or any portion of any invoice, it shall so notify Consultant within fifteen (15) days from the date of receipt of the invoice and shall pay that portion of the invoice not in dispute, and the parties shall immediately make a good faith effort to settle the disputed portion.

C. Consultant will not undertake any work or otherwise financially obligate the Agency in excess of the not-to-exceed amount in Section II(A) above without a duly authorized amendment to this Agreement.

III. Relationship of Parties

The parties intend that an independent contractor-client relationship will be created by this Agreement. As Consultant is customarily engaged in an independently established trade which encompasses the specific service provided to the Agency hereunder, no agent, employee, representative or sub-consultant of Consultant shall be or shall be deemed to be the employee, agent, representative, or sub-consultant of the Agency. In the performance of the work, Consultant is an independent contractor with the ability to control and direct the performance and details of the work, with the Agency being interested only in the results obtained under this Agreement. None of the benefits provided by the Agency to its employees including, but not limited to, compensation, insurance, and unemployment insurance are available from the Agency to the employees, agents, representatives, or sub-consultants of Consultant. Consultant will be solely and entirely responsible for its acts and for the acts of its agents, employees, representatives, and sub-consultants during the performance of this Agreement. The Agency may, during the term of this Agreement, engage other independent contractors to perform the same or similar work that Consultant performs hereunder.

IV. Duration of Agreement

This Agreement is effective as of the date it is last signed by the parties hereto, and shall remain in effect until December 31, 2020, unless terminated sooner by written notice in accordance with Section V, below.

V. Termination

A. Termination of Agreement. The Agency may terminate this Agreement for public convenience, Consultant's default, Consultant's insolvency or bankruptcy, or Consultant's assignment for the benefit of creditors, at any time prior to the expiration of this Agreement. Termination shall be effective immediately upon delivery of written notice by the Agency to Consultant, or on such date as stated in the Agency's notice, whichever is later.

B. Rights Upon Termination. In the event of termination, the Agency shall pay for all services satisfactorily performed by Consultant up to and including the effective date of termination, as described on a final invoice submitted to the Agency. Said amount shall not exceed the amount in Section II above. After termination, the Agency may take possession of all work product, records, and data within Consultant's possession pertaining to this Agreement, which records and data may be used by the Agency without restriction. Upon termination, the Agency may take over the work and prosecute the same to completion, by contract or otherwise.

VI. Discrimination

In the hiring of employees for the performance of work under this Agreement or any sub-contract hereunder, Consultant, its subcontractors, or any person acting on behalf of Consultant or its sub-consultants shall not by reason of race, religion, color, sex, national origin, or the presence of any sensory, mental, or physical disability, discriminate against any person who is qualified and available to perform the work to which the employment relates.

VII. Indemnification

Consultant shall defend, indemnify, and hold the Agency, its officers, officials, employees, agents, contractors, and volunteers harmless from any and all claims, injuries, damages, losses, or suits, including all legal costs and attorneys' fees, arising out of or in connection with the performance of this Agreement, except for injuries and damages caused by the sole negligence of the Agency. The Agency's inspection or acceptance of any of Consultant's work when completed shall not be grounds to avoid any of these covenants of indemnification. 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 Consultant and the Agency, its officers, officials, employees, agents, contractors, and/or volunteers, Consultant's liability hereunder shall be only to the extent of Consultant's negligence.

IT IS FURTHER SPECIFICALLY AND EXPRESSLY UNDERSTOOD THAT THE INDEMNIFICATION PROVIDED HEREIN CONSTITUTES CONSULTANT'S WAIVER OF IMMUNITY UNDER INDUSTRIAL INSURANCE, TITLE 51 RCW, SOLELY FOR THE PURPOSES OF THIS INDEMNIFICATION. THE PARTIES FURTHER ACKNOWLEDGE THAT THEY HAVE MUTUALLY NEGOTIATED THIS WAIVER. CONSULTANT'S WAIVER OF IMMUNITY UNDER THE PROVISIONS OF THIS SECTION DOES NOT

INCLUDE, OR EXTEND TO, ANY CLAIMS BY CONSULTANT'S EMPLOYEES DIRECTLY AGAINST CONSULTANT.

The provisions of this section shall survive the expiration or termination of this Agreement.

VIII. Insurance

A. Consultant shall procure and maintain for the duration of this Agreement, insurance against claims for injuries to persons or damage to property which may arise from or in connection with the performance of the work hereunder by Consultant, its subconsultants, agents, representatives, or employees.

B. Minimum Scope of Insurance. Consultant shall obtain insurance of the types described below:

1. Automobile Liability insurance covering all owned, non-owned, hired and leased vehicles. Coverage shall be written on Insurance Services Office (ISO) form CA 00 01 or a substitute form providing equivalent liability coverage. If necessary, the policy shall be endorsed to provide contractual liability coverage.

2. Commercial General Liability insurance shall be written on ISO occurrence form CG 00 01 or a substitute form providing equivalent liability coverage and shall cover liability arising from premises, operations, independent contractors and personal injury and advertising injury. The Agency shall be named by endorsement as an insured under Consultant's Commercial General Liability insurance policy with respect to the work performed for the Agency.

3. Workers' Compensation coverage as required by the Industrial Insurance laws of the State of Washington.

4. Professional Liability insurance appropriate to Consultant's profession.

C. Minimum Amounts of Insurance. Consultant shall maintain the following insurance limits:

1. Automobile Liability insurance with a minimum combined single limit for bodily injury and property damage of $1,000,000 per accident.

2. Commercial General Liability insurance shall be written with limits no less than $1,000,000 each occurrence, $2,000,000 general aggregate.

3. Professional Liability insurance shall be written with limits no less than $1,000,000 per claim and $1,000,000 policy aggregate limit.

D. Consultant is responsible for the payment of any deductible or self-insured retention that is required by any of Consultant's insurance. If the Agency is required to contribute to the deductible under any of Consultant's insurance policies, Consultant shall

reimburse the Agency for the full amount of the deductible within 10 working days of the Agency's deductible payment.

E. The Agency shall be named as an additional insured on Consultant's commercial general liability policy. This additional insured endorsement shall be included with evidence of insurance in the form of a Certificate of Insurance for coverage necessary in subsections B and C, above. The Agency reserves the right to receive a certified and complete copy of all of Consultant's insurance policies.

F. Consultant's insurance coverage shall be primary insurance as respects the Agency. Any insurance, self-insurance, or insurance pool coverage maintained by the Agency shall be excess of Consultant's insurance and shall not contribute with it. The Agency's own liability policy(ies) will be considered excess coverage with respect to defense and indemnity of the Agency only and no other party.

G. Consultant's insurance shall be endorsed to state that coverage shall not be cancelled by either party except after thirty (30) days' prior written notice by certified mail, return receipt requested, has been given to the Agency.

H. If any coverage is written on a "claims made" basis, then a minimum of three years' extended reporting period shall be included with the claims made policy, and proof of this extended reporting period provided to the Agency upon request.

I. Acceptability of Insurers. Consultant's insurance is to be placed with insurers with a current A.M. Best rating of not less than A:VII.

IX. Exchange of Information

The Agency warrants the accuracy of any information supplied by it to Consultant for the purpose of completion of the work under this Agreement. The parties agree that Consultant will notify the Agency of any inaccuracies in the information provided by the Agency as may be discovered in the process of performing the work, and that the Agency is entitled to rely upon any information supplied by Consultant pursuant to this Agreement.

X. Ownership and Use of Records and Documents

Original documents, drawings, designs and reports ("work product") developed under this Agreement shall belong to and become the property of the Agency. All written information submitted by the Agency to Consultant in connection with the services performed by Consultant under this Agreement will be safeguarded by Consultant to at least the same extent as Consultant safeguards like information relating to its own business. If such information is publicly available or is already in Consultant's possession or known to it, or is rightfully obtained by Consultant from third parties, Consultant shall bear no responsibility for its disclosure, inadvertent or otherwise.

XI. Agency's Right of Inspection

Even though Consultant is an independent contractor with the authority to control and direct the performance and details of the work authorized under this Agreement, the work must meet the applicable deadlines established by the Agency for completion, and the work must meet the approval of the Agency. Consultant's work shall be subject to the Agency's general right of inspection to secure the satisfactory completion thereof. Consultant agrees to comply with all federal, state, and municipal laws, rules, and regulations that are now applicable or become applicable to Consultant's business, equipment, and personnel.

XII. Consultant to Maintain Records to Support Independent Contractor Status

By the effective date of this Agreement (or shortly thereafter), Consultant shall comply with all federal and state laws applicable to independent contractors including, but not limited to the maintenance of a separate set of books and records that reflect all Items of income and expenses of Consultant's business, pursuant to the Revised Code of Washington (RCW) Section 51.08.195, as required to show that the services performed by Consultant under this Agreement do not give rise to an employer-employee relationship between the parties which is subject to RCW Title 51, Industrial Insurance.

XIII. Work Performed at Consultant's Risk

Consultant shall take all precautions necessary and shall be responsible for the safety of its employees, agents, and sub-consultants in the performance of the work hereunder and shall utilize all protection necessary for that purpose. All work shall be done at Consultant's own risk, and Consultant shall be responsible for any loss of or damage to materials, tools, or other articles used or held by Consultant for use In connection with the work.

XIV. Non-Waiver of Breach

The failure of the Agency to insist upon strict performance of any of the covenants and agreements contained herein, or to exercise any option herein conferred in one or more instances, shall not be construed to be a waiver or relinquishment of said covenants, agreements, or options and the same shall be and remain in full force and effect.

XV. Resolution of Disputes and Governing Law

Should any dispute, misunderstanding, or conflict arise as to the terms and conditions of this Agreement, the matter shall first be referred to the Program Manager of the Agency, who shall determine the term or provision's true intent or meaning. The Program Manager shall also decide all questions that may arise between the parties relative to the actual services provided or to the sufficiency or timeliness of Consultant's or Agency's performance hereunder.

If any dispute arises between the Agency and Consultant under any of the provisions of this Agreement that cannot be resolved by the Program Manager's determination in a reasonable time, or if Consultant does not agree with the Program Manager's decision on the disputed matter, then any resulting litigation must be filed in King County Superior Court, King County, Washington, which the parties agree shall be the exclusive venue for disputes relating to the interpretation, performance, or enforcement of this Agreement. This Agreement is governed by and shall be interpreted in accordance with the laws of the State of Washington, without reference to its choice-of-law rules. The non-prevailing party in any action brought to interpret or enforce this Agreement shall pay the other party's expenses, including reasonable attorney's fees.

XVI. Written Notice

Unless otherwise specified, any written notice required by this Agreement shall become effective upon the date of receipt (which may be conclusively determined by certified mail, return receipt requested, or other equivalent proof of receipt), and shall be deemed sufficiently given if delivered to the addressee at the address stated below:

CONSULTANT:

Francis & Company, PLLC
Attn: Horace Francis, CPA
200 W. Mercer St., Suite 208
Seattle, WA 98119

AGENCY:

FileLocal
Attn: Program Manager
700 Fifth Avenue, Suite 4350
Seattle, WA 98104

XVII. Assignment

Any assignment of this Agreement by Consultant without the written consent of the Agency is void. If the Agency gives its consent to any assignment, this paragraph shall continue in full force and effect and no further assignment may be made without the Agency's consent.

XVIII. Modification and Severability

No waiver, alteration, or modification of any of the provisions of this Agreement is binding unless in writing and signed by the duly authorized representatives of the Agency and Consultant.

The provisions of this Agreement are declared to be severable. If any provision of this Agreement is for any reason held to be invalid or unconstitutional by a court of competent jurisdiction, such invalidity or unconstitutionality shall not affect the validity or constitutionality of any other provision.

XIX. Entire Agreement

The written provisions and terms of this Agreement, together with any Exhibits attached hereto, supersede all prior verbal statements of any officer or other representative of the Agency, and such statements shall not be effective or be construed as entering into or forming a part of or altering in any manner whatsoever this Agreement. The entire agreement between the parties with respect to the subject matter hereunder is contained in this Agreement and any Exhibits attached hereto, which may or may not have been executed prior to the execution of this Agreement. Should any language in any of the Exhibits to this Agreement conflict with any language contained herein, then this Agreement controls.

AGREED TO AND EXECUTED BY:

CONSULTANT

By:_____
Managing Director, CEO
Francis & Company, PLLC

Date: _____

AGENCY

By:_____
Kevin Fitzpatrick, Program Manager

Date: _____

APPROVED AS TO FORM:

_____
Agency Attorney

ATTEST:

_____
Agency Secretary

EXHIBIT A

Scope of Services

Partner or Manager work with the Program Manager throughout the year as necessary to ensure that accounting and compliance issues are properly considered in the ongoing operation of the Agency. These services could include attendance at meetings with the Program Manager, Board and or Committee meetings.

Work with the Program Manager to track expenditures, verify expenditures, conduct periodic compliance monitoring, provide monthly financial statements, maintain accounting information within chart of accounts, maintain general ledger, reporting formats, internal control policies and procedures, and applicable governmental accounting requirements.

Assist with other financial and banking items such as, invoicing to cities, receipts of payments from cities, deposits to bank, bank account reconciliation and provide supporting documents for bank account along with monthly financial statements.

Work with the Program Manager to prepare annual operating budget.

Produce a full set of year-end financial statements (including management's discussion and analysis and footnotes) in accordance with generally accepted accounting principles for annual audit. Present compiled annual financial statements to management and file the annual report with the State Auditor.

EXHIBIT B

Consultant's Hourly Rates and Charges

Partner	$260
Manager	$180
Senior Accountant	$150
Staff Accountant	$115

FileLocal

File Local Resolution FL2019-02
Briefing Paper Kenyon Disend Legal Contract

Date: March 28, 2019

Issue: Shall the Washington Multi-City Business License and Tax Portal Agency ("Agency") Executive Board authorize the Program Manager to execute a contract for legal services with Kenyon Disend PLLC?

Operating Committee Recommendation: The Portal Agency Executive Board should pass Resolution FL2019-02 approving the continued use of Kenyon Disend as the Agency's legal services vendor.

Rationale: Pursuant to Section 4 of the Washington Multi-City Business License and Tax Portal Agency Interlocal Agreement, guiding principles for integrity and accountability and a goal of compliance with all applicable legal requirements were established for the Agency. The Agency contracted with Kenyon Disend as our initial law firm. The Agency believes the vendor provides a unique service due to its history and familiarity with the Agency.

RESOLUTION NO. FL2019-02

A Resolution of the Washington Multi-City Business License and Tax Portal Agency Executive Board Authorizing a Contract with Kenyon Disend PLLC to Provide Legal Services for 2019-2020.

Whereas, Pursuant to Section 4 of the Washington Multi-City Business License and Tax Portal Agency Interlocal Agreement, guiding principles for integrity and accountability and a goal of compliance with all applicable legal requirements were established for the FileLocal Agency; and

Whereas, Pursuant to Section 6 of the Washington Multi-City Business License and Tax Portal Agency Interlocal Agreement, the Executive Board of the FileLocal Agency has the power to enter into agreements with third parties for the provision of services necessary to fully implement the purposes of the Agency and the Interlocal Agreement; and

Whereas, The City of Seattle contracted with Kenyon Disend PLLC to provide legal services to the Agency during the implementation phase and during the subsequent launch period, and the Agency would like to retain Kenyon Disend as its legal services provider due to its history and familiarity with the Agency;

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 Program Manager to execute a contract with Kenyon Disend PLLC to provide legal services to the Agency as set forth in Attachment A to this Resolution.

//

//

//

//

//

//

//

ADOPTED this 28th day of March, 2019.

ATTEST:

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

Board Secretary

Board Chair

AGREEMENT FOR LEGAL SERVICES

I.
PARTIES

This Agreement is made this _____ day of _____, 2019, between the Washington Multi-City Business License and Tax Portal Agency ("Portal Agency"), and Kenyon Disend, PLLC ("Attorneys").

II.
SERVICES OF THE ATTORNEYS

Attorneys shall provide general legal services set forth in this Agreement and shall work for Portal Agency at the pleasure of and under the direction of Program Manager Kevin Fitzpatrick. David A. Linehan will direct the services provided under this Agreement.

III.
QUALITY OF SERVICES

Attorneys shall perform all legal services covered by this Agreement in a capable and efficient manner, and in accordance with the professional standards of the Washington State Bar Association.

IV.
SERVICES PROVIDED

Attorneys shall represent Portal Agency as general legal counsel. There may be occasions when Portal Agency's business requires negotiations with another city that contracts with Kenyon Disend, PLLC, to serve as that city's City Attorney. In such cases, Portal Agency understands that no lawyers at Kenyon Disend will be able to provide legal counsel to Portal Agency in connection with such negotiations. Portal Agency further understands that Kenyon Disend lawyers other than David Linehan will continue to serve the other city as its City Attorney but only on matters that are not related to the Portal Agency's negotiations with that city.

V.
FEES AND COSTS

A. Legal Services. For 2019, Portal Agency shall be billed for legal services and any necessary travel time at the Attorneys' and paralegals' hourly rates as set forth in Exhibit A. Attorneys' hourly rates for subsequent calendar years shall be provided to Portal Agency on or before November 1 of the immediately preceding calendar year. Attorneys will also charge Portal Agency fifteen cents per page for black and white photocopying and facsimile transmissions, twenty-one cents per page for color photocopying, and shall be reimbursed for legal messenger services, postage, computerized legal research charges, filing fees advanced on behalf of Portal Agency, and other direct expenses without markup.

B. Attorneys shall not charge Portal Agency for mileage reimbursement costs, nor for long-distance telephone charges.

C. Attorneys' current rates expressly account for any taxes or related charges ("charges") imposed on professional service providers by Portal Agency and State of Washington. In the event that any such additional charges are imposed during the term of this Agreement, Attorneys shall be entitled to recover any such additional charges as a reimbursable cost item on Attorneys' monthly billing statements.

VI.
PAYMENT TERMS

Fees and costs are due in full from Portal Agency upon billing by Attorneys. A service charge shall accrue at the rate of 12% per annum, but shall only be added to any balance remaining unpaid sixty (60) days after the statement date.

VII.
TIME RECORDS

Attorneys will maintain accurate time records describing the services performed and the dates upon which said services were performed, and shall provide a monthly statement to Portal Agency setting forth the time expended for such services.

VIII.
AGREEMENT PERIOD

This Agreement shall remain in effect until December 31, 2020. Each party shall have the right to terminate this Agreement upon thirty days written notice.

IX.
INSURANCE

Attorneys shall maintain for the protection of Portal Agency a professional errors and omissions insurance policy with minimum coverage of one million dollars per claim and three million dollars annual aggregate.

PORTAL AGENCY

By:_____
Kevin Fitzpatrick, Program Manager

KENYON DISEND, PLLC

By:_____
David A. Linehan, Partner

EXHIBIT A

KENYON DISEND, PLLC
HOURLY RATE SCHEDULE

ATTORNEYS:

Michael R. Kenyon	$350.00
Kim Adams Pratt	$300.00
David A. Linehan	$300.00
Hillary E. Graber	$230.00
Rachel B. Turpin	$215.00
Eileen M. Keiffer	$215.00
Ann Marie Soto	$215.00
Alexandra L. Kenyon	$165.00
Andrew D. Tsoming	$165.00

Of Counsel:

Doug F. Mosich	$300.00

PARALEGALS:

Margaret C. Starkey	$145.00
Sheryl A. Loewen	$130.00
Mary L. Maughan	$130.00
Terry T. Curran	$130.00
Antoinette M. Mattox	$120.00

FileLocal

File Local Resolution FL2019-03
Briefing Paper

Date: March 28th, 2019

Issue: Shall the Washington Multi-City Business Tax and License Portal Agency Executive Board approve the updated IT Manual?

Operating Committee Recommendation: The Portal Agency Executive Board should approve the updated IT Manual.

Rationale: The Portal Agency purpose is to provide a safe and secure technology environment for our customers. As part of its governing policy documents, the Agency develops and maintains its Portal Agency Operations Policy, including information technology security policies referred to as the IT Manual.

- Leviathan, the Agency's information technology security firm completed an audit in February 2018. The audit contained findings but none of the findings identified a significant risk, with many of them being gaps against an audit requirement. The proposed changes represent Leviathan's update to the IT Manual portion of the Portal Agency Operations Policy and clear the audit findings from the February 2018 audit.

RESOLUTION NO. FL2019-03

A Resolution of the Washington Multi-City Business License and Tax Portal Agency Executive Board Approving Amendments to the Portal Agency Operations Policy — Information Technology Security Policies (IT Manual).

Whereas, the Washington Multi-City Business License and Tax Portal Agency ("Portal Agency") Interlocal Agreement requires the development of a Portal Agency Operations Policy;

Whereas, FileLocal Resolution FL2016-04 adopted the current portions of the Portal Agency Operations Policy referred to as the IT Manual;

Whereas, the Interlocal Agreement specifies that the Operations Committee shall assist in the review of the Portal Agency Operations Policy and any amendments thereto;

Whereas, the Operations Committee has reviewed and recommends certain changes to the portions of the Portal Agency Operations Policy known as the IT Manual, as shown on Attachment A hereto; and

Whereas, approval of amendments to the Portal Agency Operations Policy requires a super-majority vote of the Executive Board;

Now Therefore,

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

SECTION 1. The Executive Board hereby approves the attached amendments to the IT Manual portion of the Portal Agency Operations Policy, as shown in Attachment A to this Resolution. For ease of reference, a "redline" of the IT Manual revisions is attached hereto as Attachment B. All previous versions of the IT Manual and any related Operations Policies that are inconsistent with the amendments shown on Attachment A are hereby repealed and replaced.

ADOPTED by super-majority vote this _____ day of _____, 2019.

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-wa.gov

Leviathan IT Policy Audit Update

March, 2019

Executive Summary

- FileLocal engaged Leviathan to assess gaps between our current practice and documented policies contained in the Operating Procedures Manual.

Engagement Summary

- To perform this engagement, LSG reviewed existing documentation to prepare for interviews with FileLocal staff. During these interviews, LSG consultants discussed process and use cases. After collecting impressions, designs and ongoing plans, LSG analyzed these results and developed a baseline. LSG compared the baseline with industry standards for governance, the ISO 27000-series security framework.

Q1'18 Summary Status

Status	Count
Agency Update	2
Annual Review - Q3'XX	6
Contractual Update	2
Leviathan	22
Passed FY2017 Audit	24
Total	56

Findings

- Review identified a number of gaps compared to best practice.
  - **None of the gaps identified constitute a significant risk to FileLocal or their customers,** with many of the gaps being gaps against an audit requirement alone.

Q1'19 Summary Status Update

Description	Count	Status
Agency Update	2	Complete
Annual Review	6	Complete - Q3 Review
Leviathan - Closed	22	Policy/Procedure Updates 3-2019
Passed FY2017 Audit	24	Closed
Subtotal - Closed	54	
Contractual Update	2	Open and will be reviewed at the conclusion of the Avenu/Kubra contracts
Leviathan - Open	0	
Subtotal - Open	2	
Total	56	

- Closed 54 Items
- Open 2 Items – two contractal

Leviathan Recommendations

As many of the gaps and recommendations in Section 3 below relate to audit requirements that an auditor or new city customer may require in order to do business with FileLocal, we have identified the following recommendations as a higher priority than the other recommendations:

• Reviewing policies and modifying them to take into account FileLocal's relationships with external agencies and vendors **– Leviathan to update in FY18**

• Determine which regular activities that are currently required by policy are necessary and which may be removed from policy or done on an as-necessary basis **– Leviathan to update in FY18**

• As necessary, document and formalize regularly performed processes to ensure consistent outcomes for high risk operations **– Leviathan to update in FY18/Q3'XX Annual Review**

• For contract renewal with Kubra and eGov, ensure that appropriate security controls are included within the contract terms and that they are written in a way that allows FileLocal to verify that such controls are effectively implemented. At a high level, these controls would include software and system testing, system patching/vulnerability management, and service level agreements on uptime **– FY 18 Contractual Updates with Kubra/eGov**

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 by the 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 across the 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

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:
    I. Confidentiality
    II. Availability
    III. Integrity requirements
    IV. Business Impact of unauthorized disclosure
D. Information Owners shall be responsible to classify the information, whose ownership has been assigned to them.
E. Users shall be responsible to manage information relative to its classification level.
F. Information shall be labelled and safeguarded relative to its classification level
G. Information labelling shall apply to information assets in physical and electronic forms
H. Information managed within FileLocal shall be classified relative to the following hierarchy and aligns to classifications adopted at a local and State level:
    I. PUBLIC
    II. SENSITIVE
    III. CONFIDENTIAL
    IV. CONFIDENTIAL, WITH SPECIAL HANDLING
I. ‘CONFIDENTIAL’ classification shall be the default classification.

J. Information shall be handled in accordance with the requirements set forth in the 'Information and Media Handling Standard'.
K. Information shall be retained in accordance with the requirements set forth in the 'Information Retention Standard'.
L. Information shall be destroyed once the applicable retention period has been exceeded.
M. 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').
N. 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.
O. 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

A. 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 regards to inappropriate information handling.
- Ensuring that all employees are trained in regards to the applied information handling controls,

B. 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.

C. 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 regards to inappropriate handling of information.

D. 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 regards 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 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 discipinary 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 regards to inappropriate personnel security.
- Ensuring that all employees are trained in regards 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 eGov 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 regards 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 access in a timely manner.
K. 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

A. 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 regards to the applied access controls to FileLocal information resources.

B. 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.

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 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 regards 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.

D. 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 regards 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.

5. Roles and Responsibilities

A. 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.

B. 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.

C. 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.

D. 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.

6. 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

7. Related Documents

- Encryption Standard

Infrastructure and Critical Vendor Policy

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 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 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

1. 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.
2. 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.
3. 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'.
4. 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.
5. All user, system, application and network activities shall be logged to the extent that provides sufficient audit trail of those activities.
6. 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.
7. All security events shall be continuously monitored.
8. All monitored and logged activity on computational resources shall be reviewed by authorized personnel.

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

5. Roles and Responsibilities

5.1. 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.

5.2. 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.

5.3. Critical Vendors (Including eGov 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 regards to the infrastructure.
- Providing periodic reports to FileLocal Agency Staffs and the FileLocal Executive with Information Security Responsibilities.

5.4. 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

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 regards 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

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 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.

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 regards 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 regards 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

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:

- 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

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 regards to media library management.
- Ensuring that appropriate personnel are trained in regards 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 regards to media library management.
- Ensuring that appropriate personnel are trained in regards 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 regards 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 regards 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 regards 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

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) 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 licence 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 regards 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 regards 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:

- 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

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.

5. 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.

D. 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

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 27002:2005:

- 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

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 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

Asset inventory records should have information such as:

- Owner
- Type
- Criticality
- Version if applicable
- 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

C. 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.

D. 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

C. 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

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:

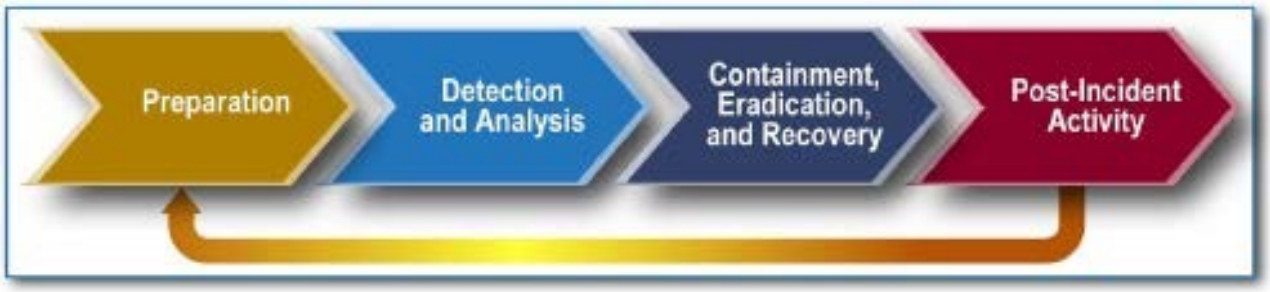


Figure 1- Security Incident Response Process

- **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

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.

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 (ie, fully qualified domain name)	Location	Description/Purpose (including criticality information)	Party Responsible/Owner	Serial Number



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 by the 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 across the 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.

Document ID:	POL-010
Reviewed by:	Operations Committee
Approved by:	<<COMPANY_APPROVER>>
Revision:	1.1
Effective Date:	<<EFFECTIVE_DATE>>

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.

Deleted: CISO, or designee.

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:
    I. Confidentiality
    II. Availability
    III. Integrity requirements
    IV. Business Impact of unauthorized disclosure
D. Information Owners shall be responsible to classify the information, whose ownership has been assigned to them.
E. Users shall be responsible to manage information relative to its classification level.
F. Information shall be labelled and safeguarded relative to its classification level
G. Information labelling shall apply to information assets in physical and electronic forms
H. Information managed within FileLocal shall be classified relative to the following hierarchy and aligns to classifications adopted at a local and State level:
    I. PUBLIC
    II. SENSITIVE
    III. CONFIDENTIAL
    IV. CONFIDENTIAL, WITH SPECIAL HANDLING
I. 'CONFIDENTIAL' classification shall be the default classification.

J. Information shall be handled in accordance with the requirements set forth in the 'Information and Media Handling Standard'.
K. Information shall be retained in accordance with the requirements set forth in the 'Information Retention Standard'.
L. Information shall be destroyed once the applicable retention period has been exceeded.
M. 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').
N. 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.
O. 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

A. 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 regards to inappropriate information handling.
- Ensuring that all employees are trained in regards to the applied information handling controls,

Deleted: <#>FileLocal Executive with Information Security responsibilities¶
<#>The Chief Information Security Officer (CISO or in lieu of a dedicated CISO, the member of executive who is ultimately responsible for information security, is responsible for:¶

B. 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.

C. 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 regards to inappropriate handling of information.

Deleted: CISO

Deleted: CISO

D. 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 regards 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.

Deleted: CISO

Deleted: CISO

Deleted: CISO

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

Deleted: 2005

Deleted: 4.1 – Assessing Security Risks ¶
Section 7

Deleted: 7

Deleted: 7

Deleted: 7

Deleted: Information

Deleted: and

Deleted: 10.7

Deleted: 10.7.3 – Information Handling Procedures ¶
Section 10.

Deleted: in Transit

Deleted: 10.8.4

Deleted: 12.3 – Cryptographic Controls ¶
Section 15

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 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 discipinary 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 regards to inappropriate personnel security.
- Ensuring that all employees are trained in regards 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 eGov 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 regards 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

Document ID: POL-020

Reviewed by: Operations Committee
Approved by: <<COMPANY_APPROVER>>

Revision: 1.1
Effective Date: <<EFFECTIVE_DATE>>

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 access in a timely manner.
K. 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.

Deleted:

Deleted: Executive with Information Security responsibilities.

- **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

A. 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 regards to the applied access controls to FileLocal information resources.

B. 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.

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 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 regards 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.

D. 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.

Deleted: <#>FileLocal Executive with Information Security responsibilities¶
<#>Executive with Information Security responsibilities

Deleted: CISO, OR

Deleted: breaches

Deleted: CISO

Deleted: CISO

Deleted: CISO

- 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 regards 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.

Deleted: FileLocal

Deleted: CISO

Deleted: FileLocal

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

Deleted: 2005

Deleted: 3 – Allocation of

Deleted: 8

Deleted: 10

Deleted: 3

Deleted: 11

7. Related Documents

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

Document ID:	POL-030
Reviewed by:	Operations Committee
Approved by:	<<COMPANY_APPROVER>>
Revision:	1.1
Effective Date:	<<EFFECTIVE_DATE>>

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.

Deleted: Chief Information Security Officer (CISO), or designee….

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.

5. Roles and Responsibilities

A. 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.

Deleted: <#>FileLocal Executive with Information Security responsibilities¶
<#>FileLocal Executive with Information Security responsibilities…

B. 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.

C. 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.

D. 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.

6. 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

7. Related Documents

- Encryption Standard

Deleted: Executive with Information Security Responsibilities…

Deleted: Promptly reporting security incidents to Help Desk…

Deleted: to

Deleted: , in accordance to the Information Security Policies adopted…

Deleted: <#>Co-operating with and contributing to the security incident response activities as required. ¶

Deleted: Incident Response

Deleted: 2005

Deleted: 4

Deleted: Assessing Security Risks ¶
Section 6.1.6 – Contact with Authorities ¶
Section 6.2.3 – Addressing security in third party agreements ¶
Section 7.2.1 – Classification guidelines

Deleted: .1 – Reporting information security events

Deleted: Responsibilities

Deleted: procedures

Deleted: 2.2 – Learning from information security incidents…

Deleted: 13.2.3 – Collection of evidence

Deleted: Incident Response

Deleted:

Document ID: POL-040

Reviewed by: Operations Committee
Approved by:

Revision: 1.1
Effective Date: <<EFFECTIVE_DATE>>

Infrastructure and Critical Vendor Policy

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.

Deleted: File Local
Deleted: File Local
Deleted: shareholder value.
Deleted: ,

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 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.

Deleted: File Local's
Deleted: File Local's

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:

Deleted: File Local

- Full-time employees
- Part-time employees
- Temporary supplemental staff
- Contractors
- Consultants
- Vendors, including, but not limited to, eGov 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.

Deleted: File Local
Deleted: File Local

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.

Deleted: File Local
Deleted: File Local Executive with Information Security Responsibilities…

4. Policy Statements

1. 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.
2. 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.
3. 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'.
4. 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.
5. All user, system, application and network activities shall be logged to the extent that provides sufficient audit trail of those activities.
6. 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.
7. All security events shall be continuously monitored.
8. All monitored and logged activity on computational resources shall be reviewed by authorized personnel.

Deleted: File Local
Deleted: File Local's
Deleted: File Local's
Deleted: File Local's

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

5. Roles and Responsibilities

5.1. 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.

5.2. 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.

5.3. Critical Vendors (Including eGov 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 regards to the infrastructure.
- Providing periodic reports to FileLocal Agency Staffs and the FileLocal Executive with Information Security Responsibilities.

Deleted: <#> File Local Executive with Information Security Responsibilities¶
<#>The File Local Executive with Information Security Responsibilities…

Deleted: File Local's

Deleted: File Local's

Deleted: File Local's

Deleted: File Local

Deleted: File Local

Deleted: File Local's

Deleted: File Local

Deleted: File Local

Deleted: File Local

Deleted: File Local

Deleted: File Local

Deleted: File Local

Deleted: File Local

Deleted: File Local

Deleted: File Local

Deleted: File Local

5.4. 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.

Deleted: File Local's

Deleted: File Local's

Deleted: File Local's

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

Document ID: POL-050

Reviewed by: Operations Committee
Approved by: <<COMPANY_APPROVER>>

Revision: 1.1
Effective Date: <<EFFECTIVE_DATE>>

Physical and Environmental Security Policy

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.

Deleted: Executive with Information Security responsibilities.

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".

Deleted: apply physical security in depth (that is, layering defences like fences, alarms, manned reception area, and locks) as appropriate to the specific facility. ¶
FileLocal shall apply

Deleted: apply

Deleted: <#>Still image, video cameras, and any other electronic recording devices shall be prohibited in restricted areas. Special attention shall be taken with visitors carrying cell phones equipped with digital cameras. ¶

Deleted: <#>Doors and windows of restricted areas shall be locked when unattended, and external protection shall be considered for windows on the ground floor. ¶

5. Roles and Responsibilities

A. Program Manager

The Program Manager is responsible for:

Deleted: <#>FileLocal Executive with Information Security responsibilities¶
<#>Executive with Information Security responsibilities

- Performing organizational self-assessment periodically to ensure compliance with this policy and related standard.
- Ensuring that all employees are trained in regards 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

Deleted: 2005

Deleted: 4.1 – Assessing Security Risks¶
Section 4.2 – Treating Security Risks¶
Section 9

Deleted: 9

Deleted: 9

Deleted: 9

Deleted: 9

Deleted: 9

Deleted: sitting

Deleted: 9

Deleted: 9

Deleted: 7

Deleted: 3.3

Deleted: Physical and Environmental Standard

Document ID: POL-060

Reviewed by: Operations Committee
Approved by: <<COMPANY_APPROVER>>

Revision: 1.1
Effective Date: <<EFFECTIVE_DATE>>

Third Party Management and Outsourced Services Policy

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.

Deleted: File Local's

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:

Deleted: File Local

- 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.

Deleted: File Local

Deleted: File Local

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.

Deleted: File Local

Deleted: File Local

Deleted: File Local

Deleted: File Local

Deleted: File Local

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.

Deleted: Executive with Information Security responsibilities

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.

Deleted: File Local's

- 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.

Deleted: File Local
Deleted: File Local's
Deleted: File Local's
Deleted: File Local's
Deleted: File Local
Deleted: File Local
Deleted: File Local's
Deleted: File Local's

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 regards to Third Party access control breaches.

Deleted: <#>Executive with Information Security responsibilities¶
<#>The Executive with Information Security responsibilities
Deleted: File Local

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.

Deleted: <#>File Local ¶
<#>File Local

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.

Deleted: Information Custodians
Deleted: File Local

- 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 regards 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
-

Deleted: File Local

Deleted: File Local

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

Deleted:

7. Related Documents

- N/A

DATA BACKUP

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:

- 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

Document ID: POL-080

Reviewed by: Operations Committee
Approved by: <<COMPANY_APPROVER>>

Revision: 1.1
Effective Date: <<EFFECTIVE_DATE>>

Data Storage Media Library Management Policy

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 regards to media library management.
- Ensuring that appropriate personnel are trained in regards to the applied media library management controls.

Deleted: Executive with Information Security responsibilities

Deleted: <#>FileLocal shall adopt formal procedures for the management, handling, and storage of removable data storage media (for example, tapes, disks, and cassettes). ¶

Deleted: <#>the

Deleted: C.

Deleted: re-usable

Deleted: <#>FileLocal shall keep a formal record of all activities conducted with removable data storage media, including new media added to the library, transfer to remote locations, and media removal. These records shall include the dates, approvals, and details of each activity, so that FileLocal is able to trace every step on the media life cycle. ¶
<#>FileLocal shall control access to removable data storage media in accordance Access Control Policy and related Standards. ¶

Deleted: <#>FileLocal Executive with Information Security responsibilities¶
<#>Executive with Information Security responsibilities

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 regards to media library management.
- Ensuring that appropriate personnel are trained in regards 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 regards 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 regards 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 regards 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

Deleted:

Deleted: 2005

Deleted: 7

Deleted: 7

Deleted: 7

Deleted: Information labelling and handling

Deleted: 9

Deleted: 7

Deleted: property

Deleted: 10.7

Deleted: 10.7

Deleted: <#>Section 10.7.3 – Information handling procedures ¶

Deleted: <#>10.10

Deleted: 11

7. Related Documents

- N/A

COMPLIANCE

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) 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 licence 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 regards 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 regards 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:

- 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

Document ID:	POL-100
Reviewed by:	Operations Committee
Approved by:	<<COMPANY_APPROVER>>
Revision:	1.1
Effective Date:	<<EFFECTIVE_DATE>>

Incident Response Policy

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.

Deleted: Executive with Information Security responsibilities.

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.

5. 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.

Deleted: Executive with Information Security responsibilities. …

Deleted: Executive with Information Security responsibilities…

Deleted: <#>Executive with Information Security responsibilities¶
<#>Executive with Information Security responsibilities

Deleted:

Deleted:

Deleted:

Deleted:

Deleted:

Deleted:

Formatted: Bulleted + Level: 1 + Aligned at: 0.75" + Indent at: 1", Tab stops: 0.75", List tab

Moved down [1]: Assessing, categorizing and analyzing security incidents.

Moved down [3]: Directing the Computer Security Incident Response Team.

Deleted:

Moved down [4]: Escalating security incidents as necessary.

Moved down [6]: Ensuring the cause of security incidents has been identified and addressed.

Deleted:

Moved down [5]: Providing recommendations to resolve security incidents.

Moved down [7]: Ensuring security incidents are resolved. ¶

Deleted:

Moved down [2]: Leading security investigations.

Deleted:

Deleted:

Deleted:

Deleted:

Moved (insertion) [1]

Moved (insertion) [2]

Moved (insertion) [3]

Moved (insertion) [4]

- 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.

D. 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

Moved (insertion) [5]

Moved (insertion) [6]

Moved (insertion) [7]

Deleted: ¶

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

Deleted: 2005:

Formatted: Font: Arial

Formatted: Space After: 10 pt

Deleted: <#>Section 4.1 – Assessing Security Risks ¶

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.5" + Indent at: 0.75"

Formatted: Font: Arial

Deleted: <#>6

Formatted: Font: Arial

Formatted: List Paragraph, Space Before: 0 pt, After: 0 pt, Bulleted + Level: 1 + Aligned at: 0.5" + Indent at: 0.75"

Deleted: 6

Formatted: Font: Arial

Deleted: .3

Formatted: Font: Arial

Deleted: in third party

Formatted: Font: Arial

Deleted: 7

Formatted: Font: Arial

Deleted: guidelines

Formatted: Font: Arial

Formatted: Font: Arial

Formatted: List Paragraph, Space Before: 0 pt, After: 0 pt, Bulleted + Level: 1 + Aligned at: 0.5" + Indent at: 0.75"

Deleted: 13

Formatted: Font: Arial

Deleted: 1

Formatted: Font: Arial

Deleted: 13.2.1 – Responsibilities and procedures ¶ Section 13.2.2 –

Formatted: Font: Arial

Deleted: 13.2.3

Formatted: Font: Arial

Formatted: Font: Arial, 9 pt

Formatted: Font: Arial, 9 pt

Deleted: N/A

SECURITY RISK ASSESSMENT

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 27002:2005:

- Section 4 – Risk Assessment and Treatment

7. Related Documents

- PRO-310 Risk Management Process

Document ID: POL-130

Reviewed by: Operations Committee
Approved by: <<COMPANY_APPROVER>>

Revision: 1.1
Effective Date: <<EFFECTIVE_DATE>>

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.

Deleted: Executive with Information Security responsibilities.

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

Deleted: <#>Executive with Information Security responsibilities¶
<#>Executive with Information Security responsibilities

Deleted: <#>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 regards to the applied access controls to FileLocal information resources. ¶
<#>¶
<#>FileLocal Agency ¶

Deleted: <#>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 ... [1]

Deleted: <#>that users of their resources

Deleted: <#>complying

Deleted: <#> and the associated standard and ... [2]

Deleted: security controls that are mandated by this ... [3]

Deleted: systems of which they are in charge. ¶

Deleted: CISO, OR designee's organizational self- ... [4]

Deleted: computational environment's components ... [5]

Deleted: CISO, or designee, in investigations in regards ... [6]

Deleted: <#>Monitoring access control activities. ¶ ... [7]

Deleted: Accessing only the information resources

Formatted ... [8]

Deleted: which they have been granted permission. ¶ ... [9]

Deleted: related

Deleted: (e.g. unauthorized access) to FileLocal and a ... [10]

Deleted: Access Control

Deleted: 2005

Formatted ... [11]

Deleted: 6

Deleted: 3 – Allocation of Information Security ... [12]

Deleted: 8.2.1 – Management Responsibilities

Deleted: <#>Section 10.1.3 – Segregation of Duties ¶ [13]

Deleted: Access Control

Formatted ... [14]

Deleted: ¶ ... [15]

Document ID:	POL-140
Reviewed by:	Operations Committee
Approved by:	<<COMPANY_APPROVER>>
Revision:	1.1
Effective Date:	<<EFFECTIVE_DATE>>

Business Continuity Policy

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.

Deleted: Executive with Information Security responsibilities.

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

Deleted: <#>Executive with Information Security responsibilities¶
<#>Executive with Information Security responsibilities

Deleted: 2005

Deleted: 14 –

Deleted: N/A

Document ID: GDE-200

Reviewed by: Operations Committee
Approved by: <<COMPANY_APPROVER>>

Revision: 1.1
Effective Date: <<EFFECTIVE_DATE>>

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.

Moved down [1]: <#>Introduction¶

2. VENDOR RESPONSIBILITIES

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

Deleted: are usually the business unit leaders (e.g. VP, EVP, AVP)….

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

Asset inventory records should have information such as:

- Owner
- Type
- Criticality
- Version if applicable
- 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

C. 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.

D. 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

Formatted: Font: Not Bold

Moved (insertion) [2]

Formatted: List Paragraph

Moved up [2]: <#>Keep terminated User information (e.g. files, e-mails) for 30 days. ¶

Deleted: removable

Deleted: removable

  - 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

Deleted:
Deleted:
Deleted:
Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 1" + Indent at: 1.25"

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

C. 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

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

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.

Formatted: Section start: Continuous

11. Asset Inventory

Moved (insertion) [1]

11.1. Introduction

Formatted: Heading 2

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 domain name)	Location	Description/Purpose (including criticality information)	Party Responsible/Owner	Serial Number

Formatted: Font: Arial, 9 pt

Formatted: Indent: Left: 0", Space Before: 0 pt, After: 10 pt

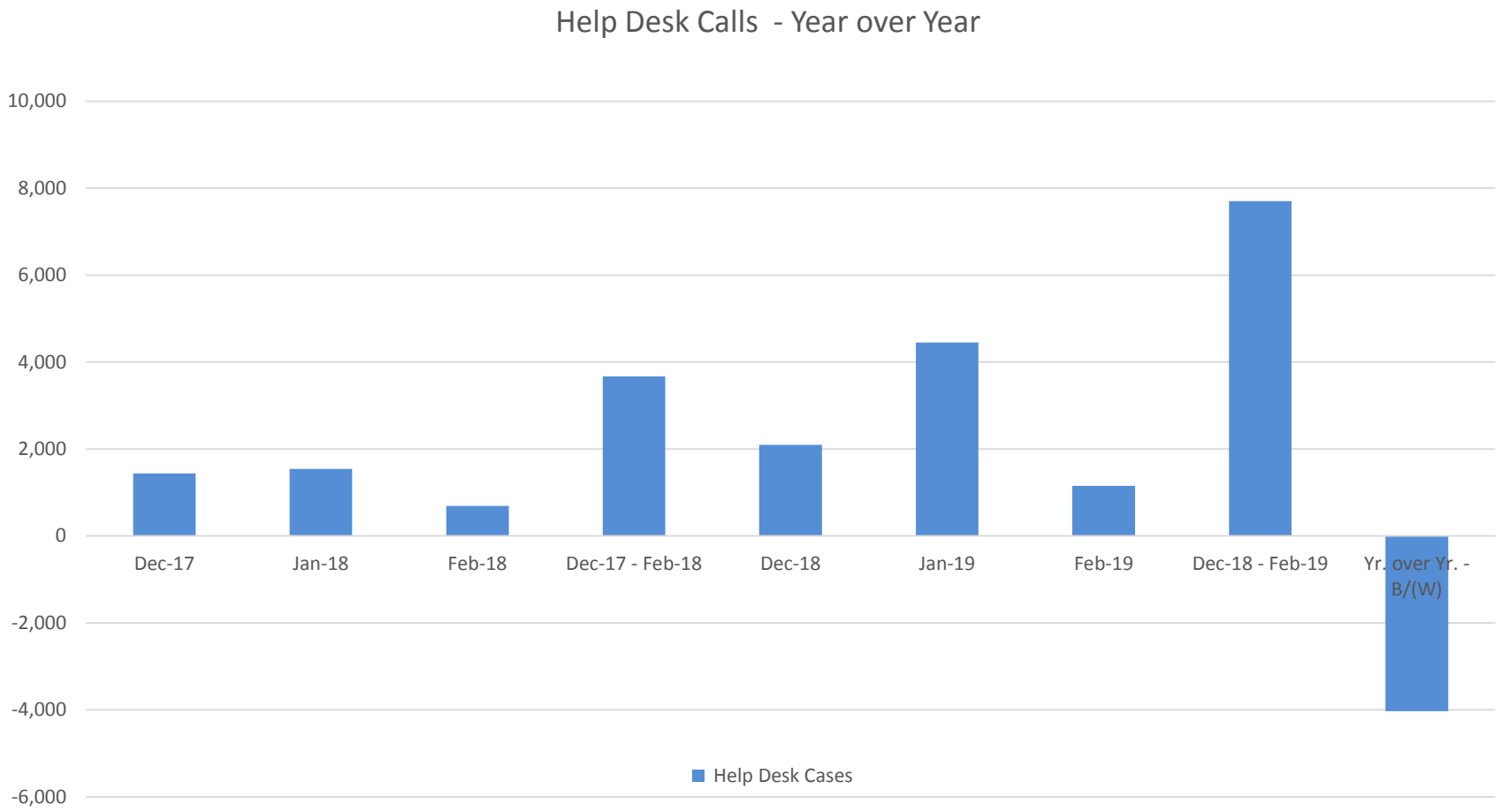
FileLocal

Your one stop for local business licensing and tax filing

www.filelocal-wa.gov

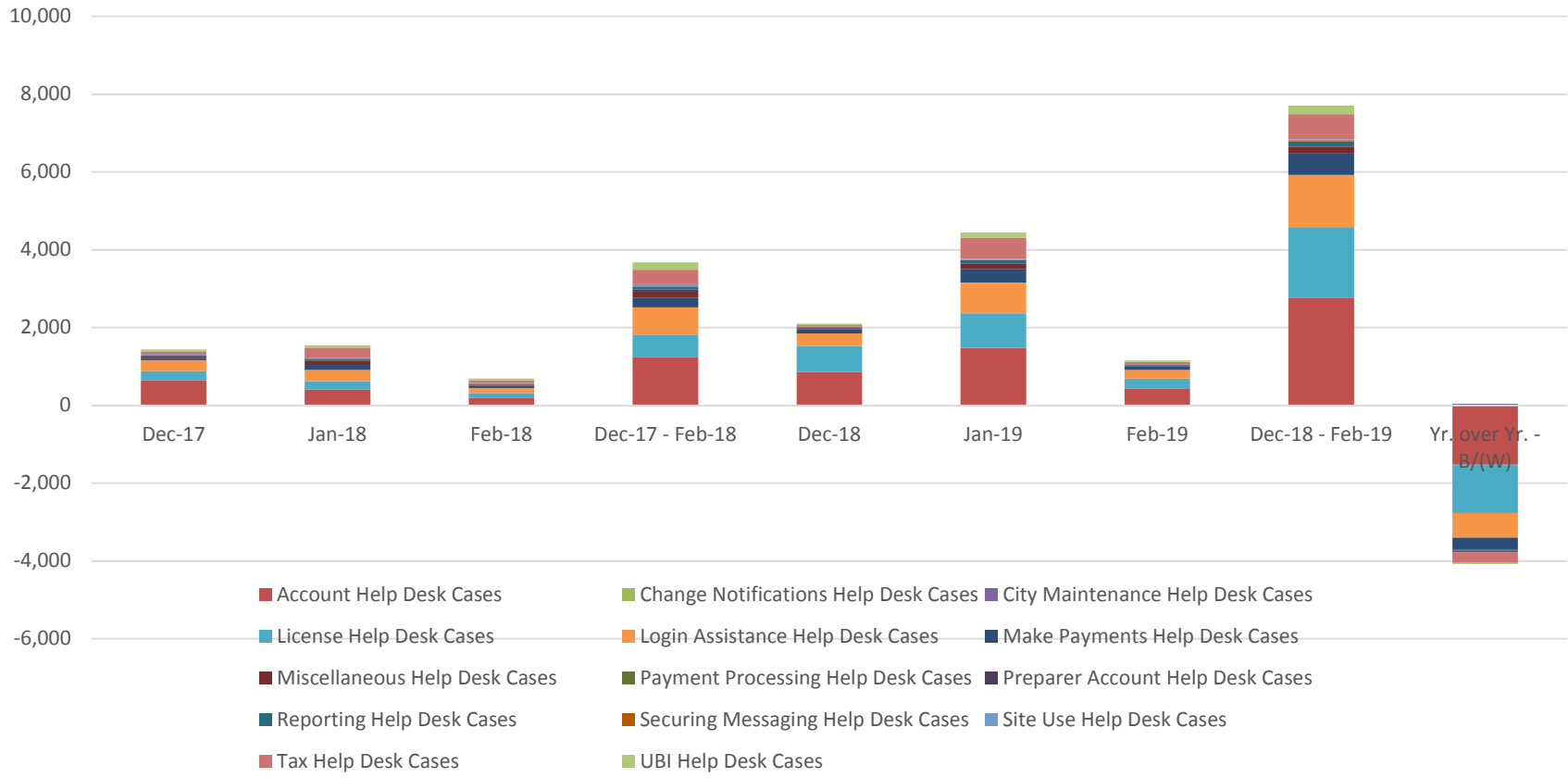
FileLocal: Monthly Business Review

February 2019

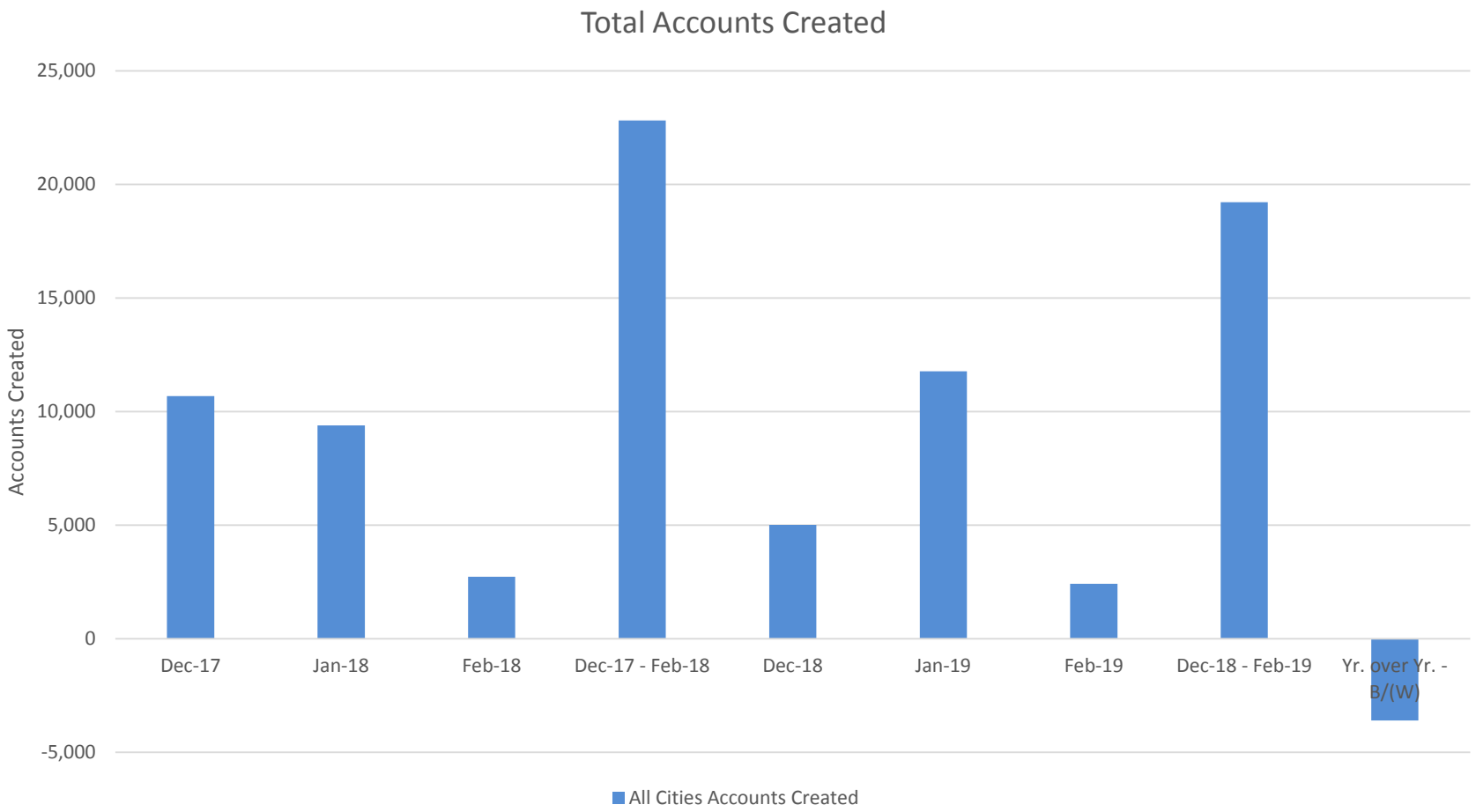


Help Desk Calls by Functional Category	Help desk calls totaled 7,705 for the three months ending February 2019. This is 12.7% of the accounts created and transactions processed which is 4.1% higher than the same three months in the prior year (8.5%). Compared to the prior year, the number of calls were up 4,031. Three categories make up the highest (75%) % of calls - account creation (36%), licenses (23%) and login (17%). The increase in calls is primarily related to questions on renewals. Total renewals grew from 8,343 to 13,732.

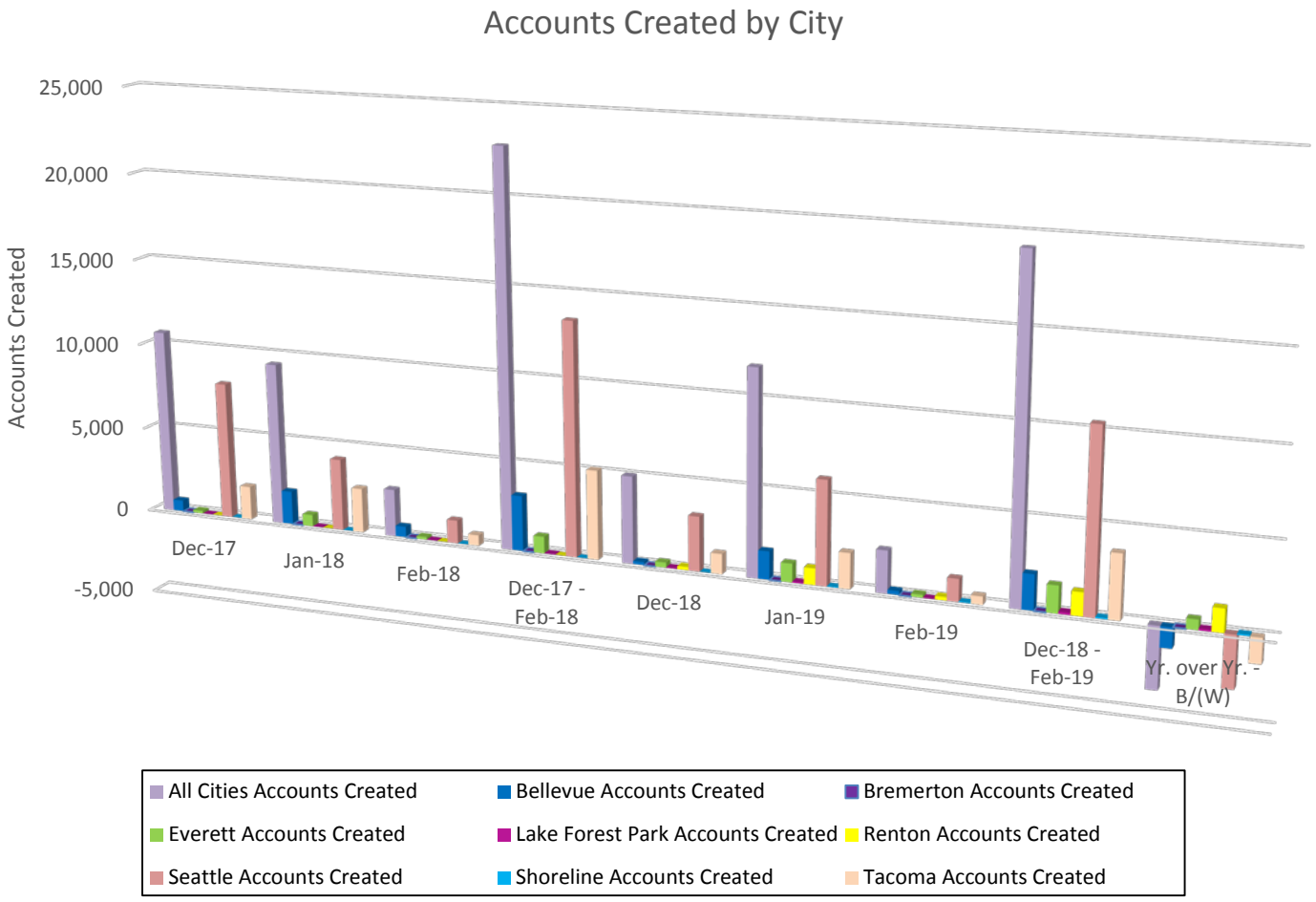
Help Desk Calls by Functional Category - Year over Year



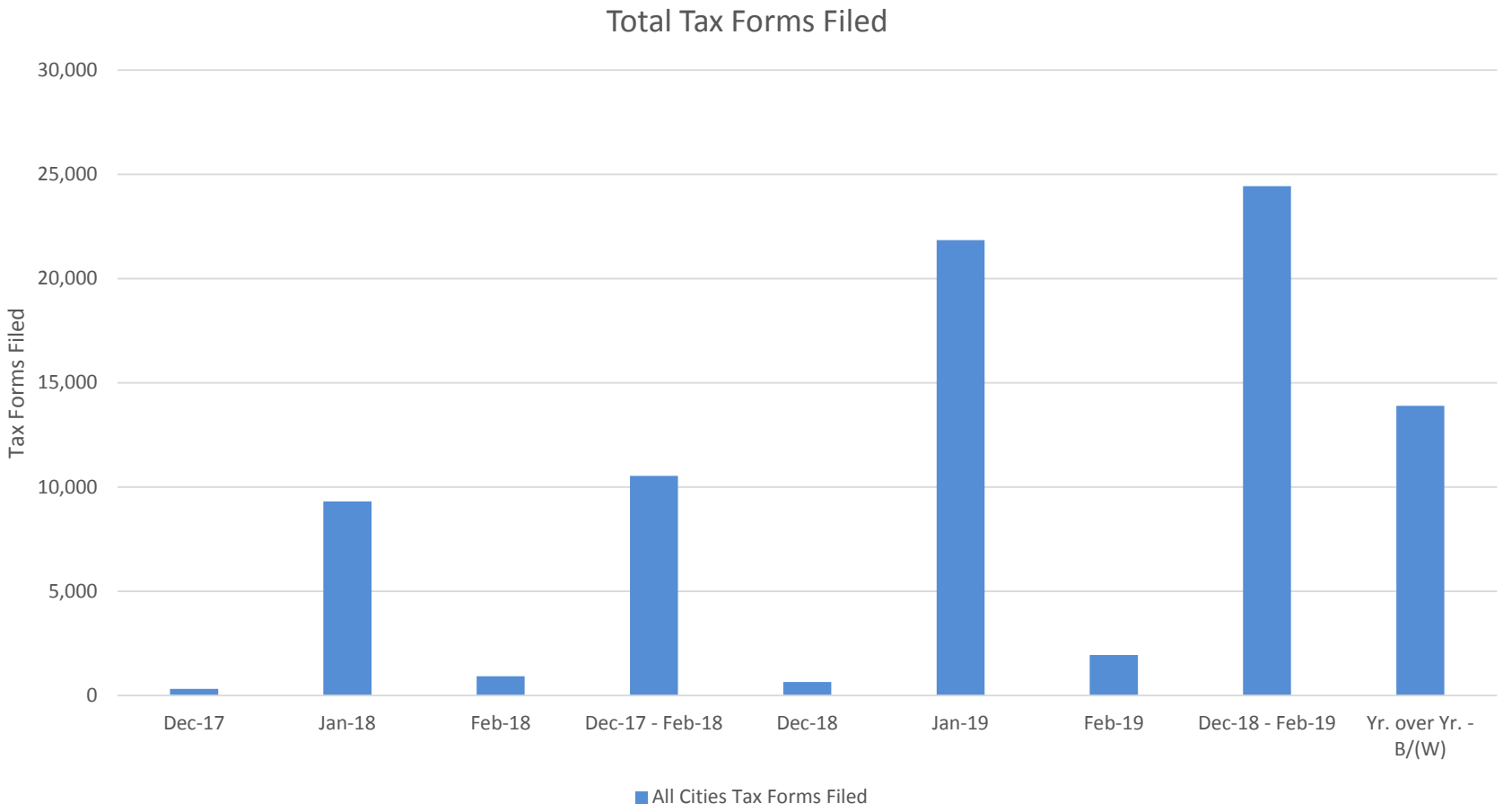
Help Desk Calls by Functional Category	Help desk calls totaled 7,705 for the three months ending Febuary 2019. This is 12.7% of the accounts created and transactions processed which is 4.1% higher than the same three months in the prior year (8.5%). Compared to the prior year, the number of calls were up 4,031. Three categories make up the highest (75%) % of calls - account creation (36%), licenses (23%) and login (17%). The increase in calls is primarily related to questions on renewals. Total renewals grew from 8,343 to 13,732.



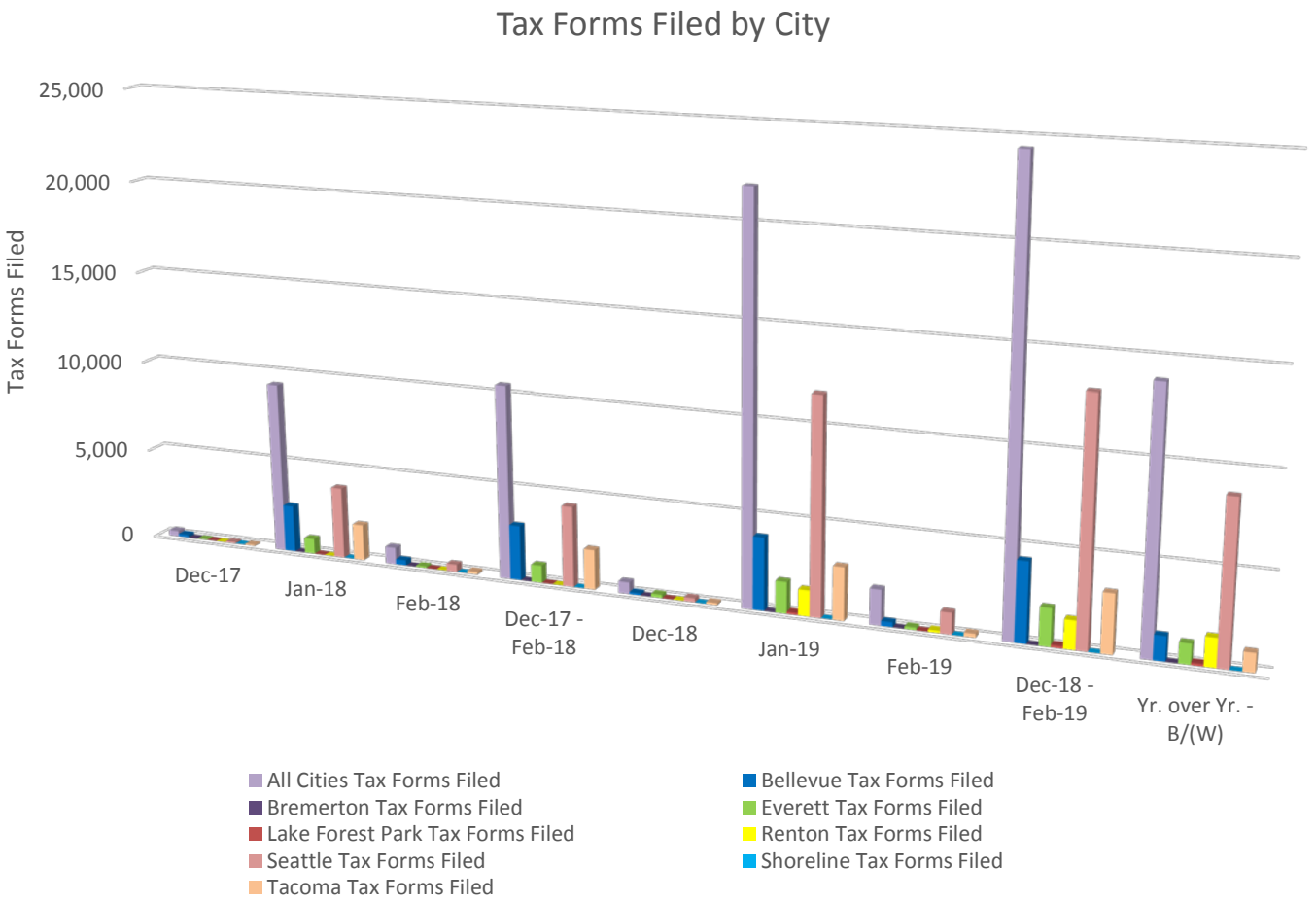
Accounts Created	Accounts created for the 3 months ended February 2019 were 19,223 which is down 3,592 accounts compared to the same 3 months in the prior year. Three of the eight cities were down with Bellevue down 1,186, Bremerton flat, Everett up 580, Lake Forest Park up 100, Renton up 1,340, Seattle down 3,033, Shoreline up 74 and Tacoma down 1,467.



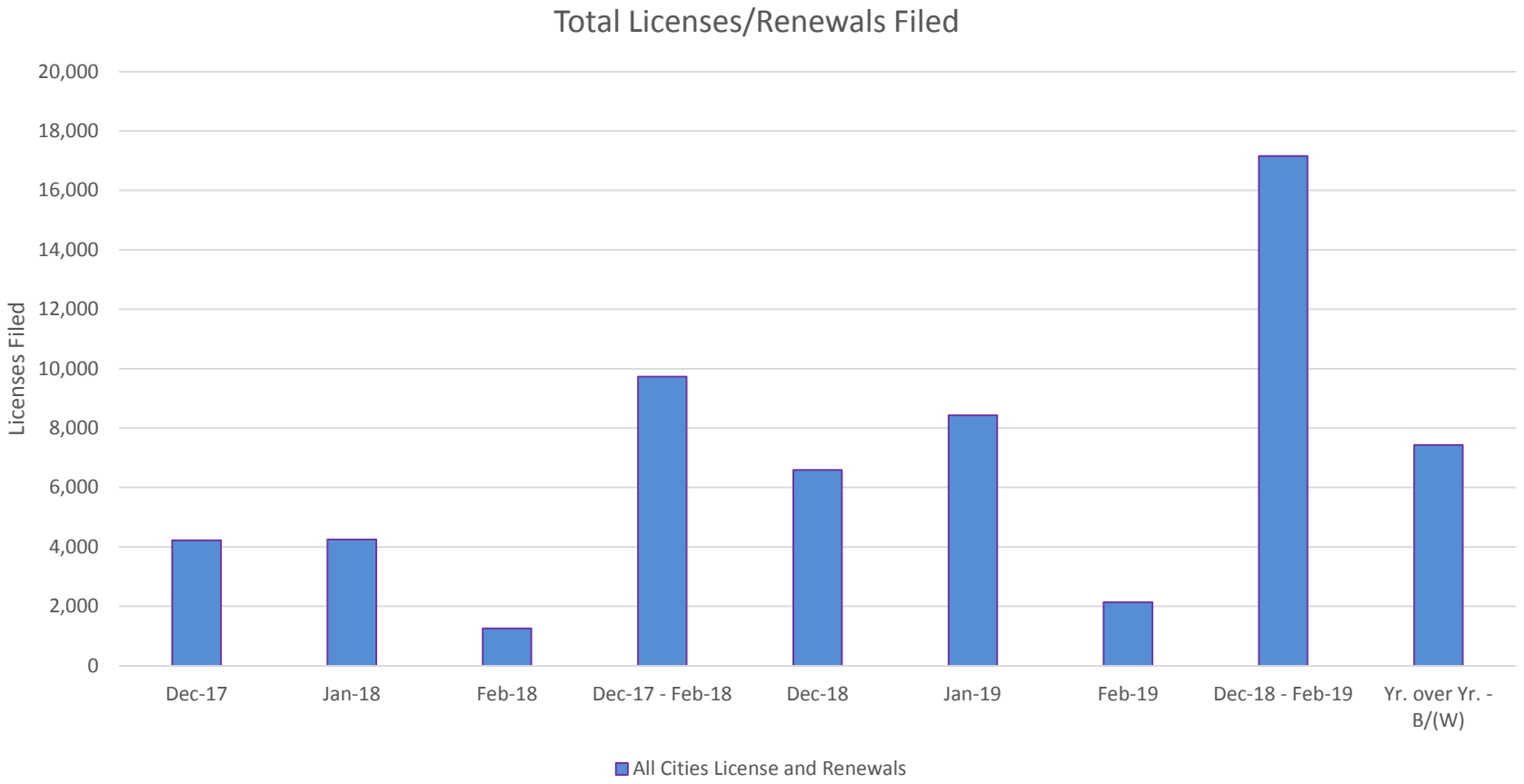
Accounts Created	Accounts created for the 3 months ended February 2019 were 19,223 which is down 3,592 accounts compared to the same 3 months in the prior year. Three of the eight cities were down with Bellevue down 1,186, Bremerton flat, Everett up 580, Lake Forest Park up 100, Renton up 1,340, Seattle down 3,033, Shoreline up 74 and Tacoma down 1,467.



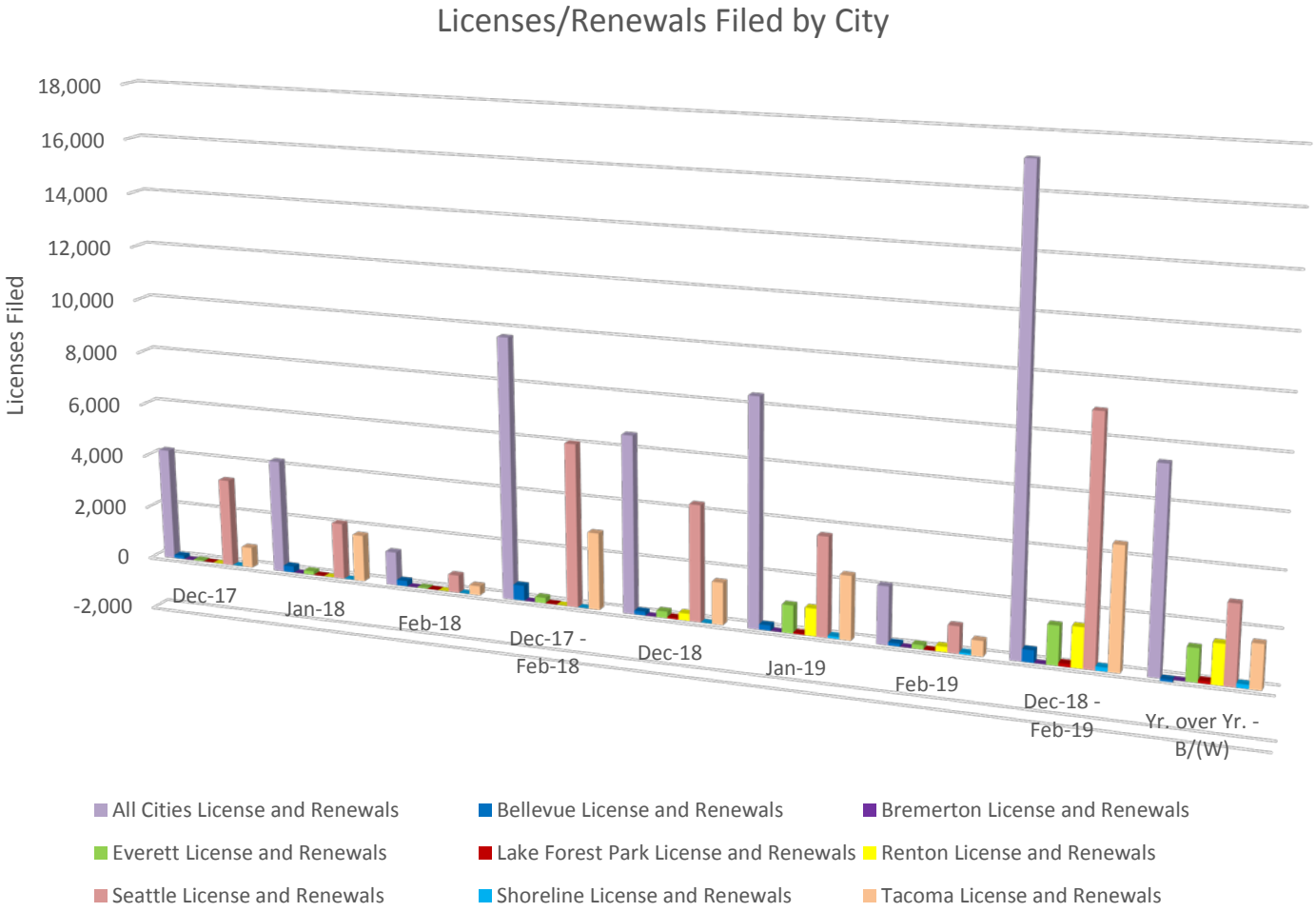
Tax Forms Filed	Tax Forms filed for the 3 months ended Febuary 2019 were 24,432 which is up 13,899 filings compared to the same 3 months from the prior year. Seven of the eight cities were up with Bellevue up 1,338, Bremerton flat, Everett up 1,110, Lake Forest Park up 132, Renton up 1,569, Seattle up 8,709 and Tacoma up 1,041. Forms with $0 liability were 12,408 which is up 6,350 from the same three months of the prior year and represent 30% of the total transactions.



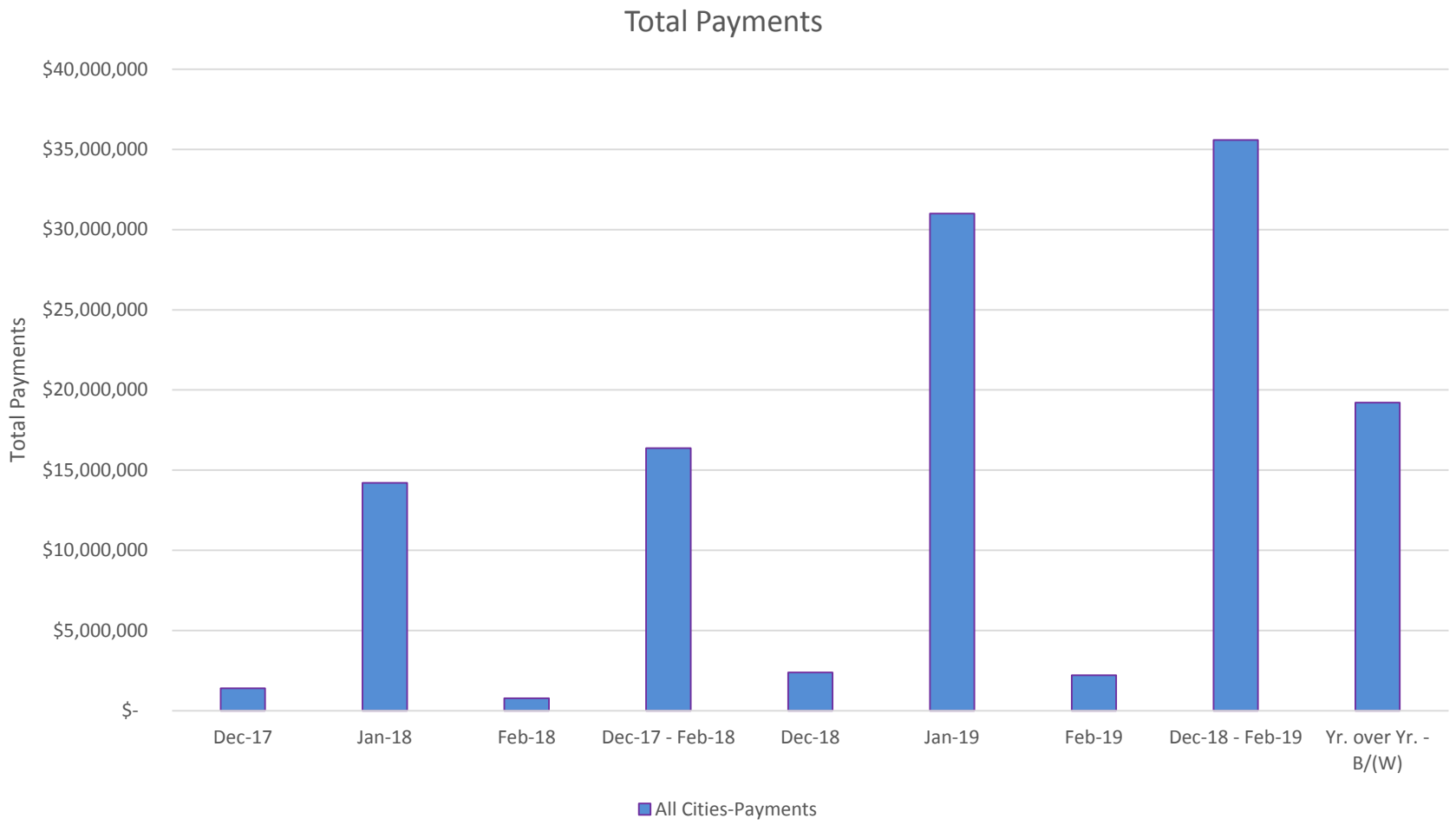
Tax Forms Filed	Tax Forms filed for the 3 months ended Febuary 2019 were 24,432 which is up 13,899 filings compared to the same 3 months from the prior year. Seven of the eight cities were up with Bellevue up 1,338, Bremerton flat, Everett up 1,110, Lake Forest Park up 132, Renton up 1,569, Seattle up 8,709 and Tacoma up 1,041. Forms with $0 liability were 12,408 which is up 6,350 from the same three months of the prior year and represent 30% of the total transactions.



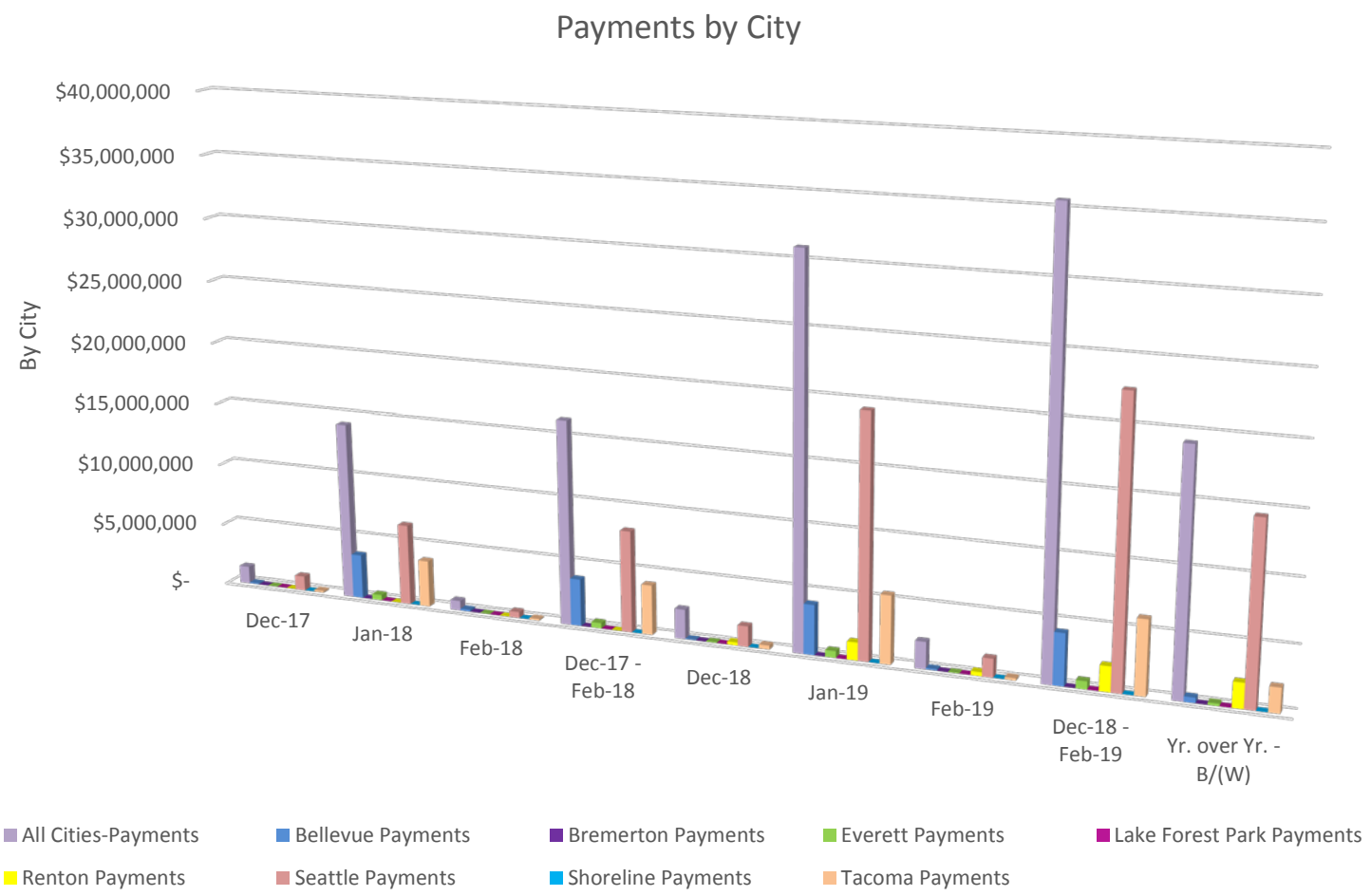
Licenses/Renewals Filed	License/Renewals created for the 3 months ended February 2019 were 17,159 which is up 7,431 filings compared to the same 3 months from the prior year. Six of the eight cities were up with Bellevue down 110, Bremerton flat, Everett up 1,232, Lake Forest Park up 102, Renton up 1,486, Seattle up 2,928, Shoreline up 154 and Tacoma up 1,639.



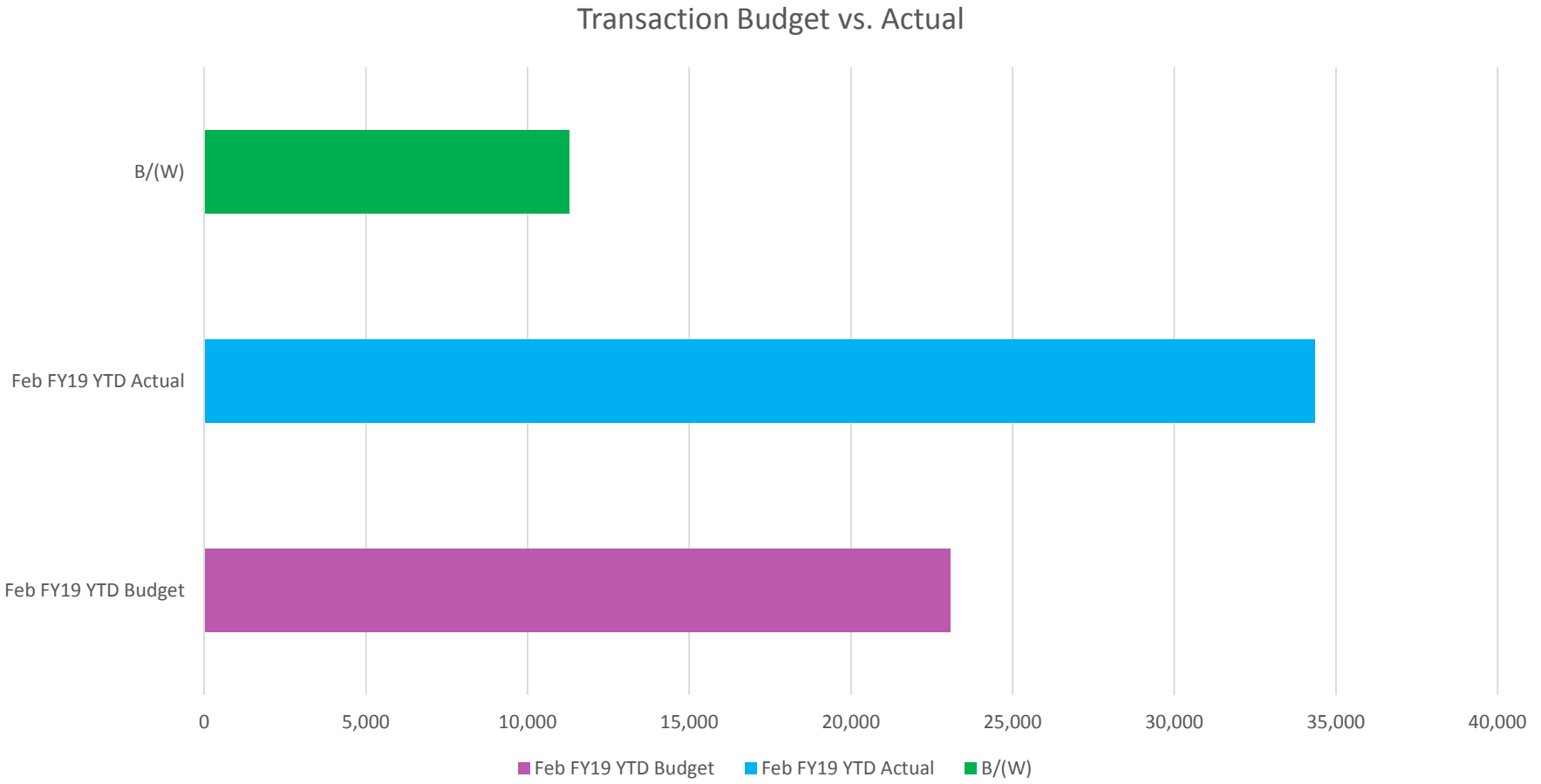
Licenses/Renewals Filed	License/Renewals created for the 3 months ended February 2019 were 17,159 which is up 7,431 filings compared to the same 3 months from the prior year. Six of the eight cities were up with Bellevue down 110, Bremerton flat, Everett up 1,232, Lake Forest Park up 102, Renton up 1,486, Seattle up 2,928, Shoreline up 154 and Tacoma up 1,639.



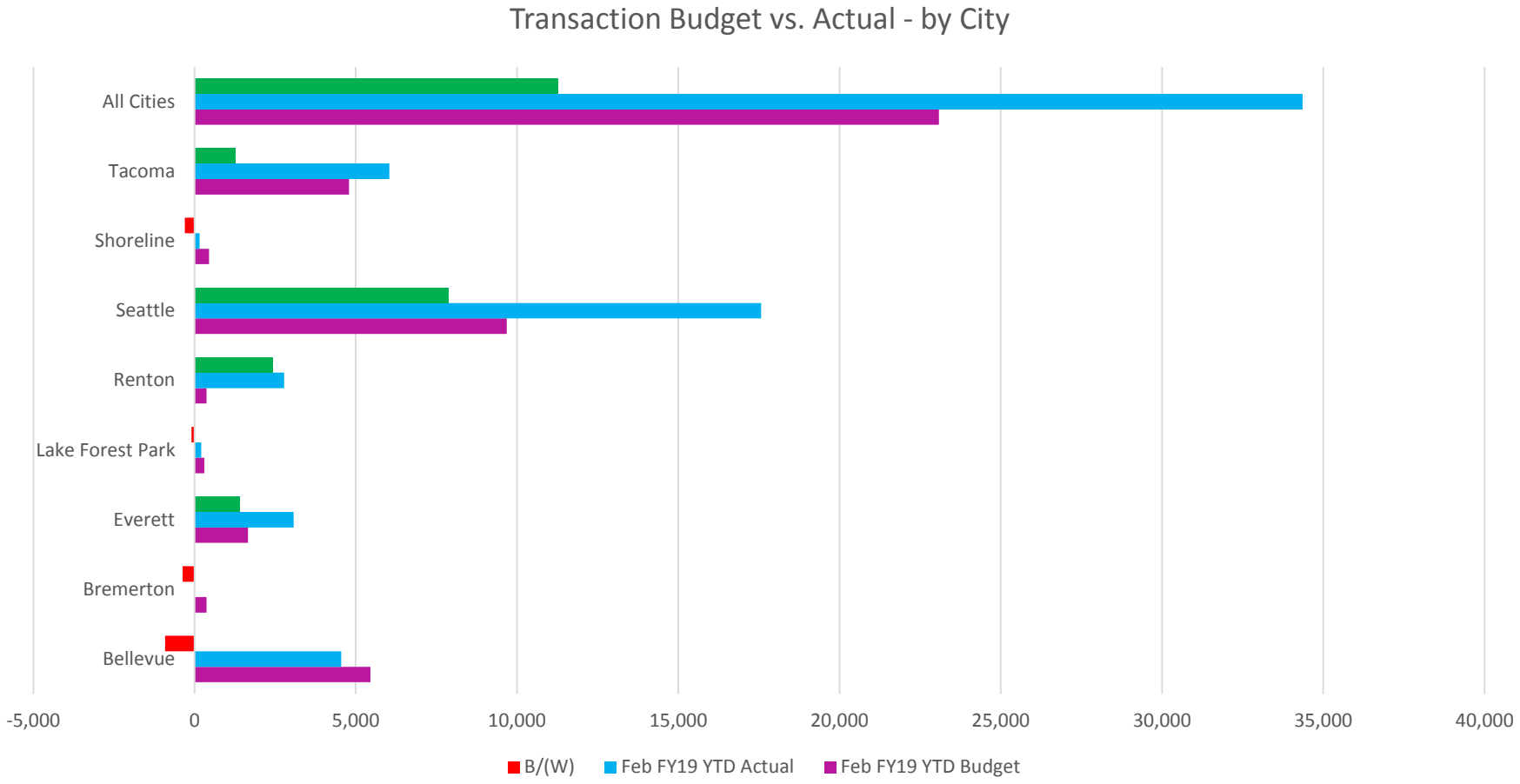
Payments Made by City	Payments made for the 3 months ended February 2019 were $35,591m which is up $19.217m compared to the same 3 months from the prior year. Seven of the eight cities were up with Bellevue up $440k, Bremerton flat, Everett up $206k, Lake Forest Park up $20k, Renton up $2,057k, Seattle up $14,458k, Shoreline up $6k and Tacoma up $2,030k.



Payments Made by City	Payments made for the 3 months ended February 2019 were $35,591m which is up $19.217m compared to the same 3 months from the prior year. Seven of the eight cities were up with Bellevue up $440k, Bremerton flat, Everett up $206k, Lake Forest Park up $20k, Renton up $2,057k, Seattle up $14,458k, Shoreline up $6k and Tacoma up $2,030k.



Transactions YTD Budget versus YTD Actual	Transactions YTD Budget versus Actual were favorable by 11,280. Three cities were favorable and four cities were unfavorable. Bellevue was unfavorable by 912, Bremerton was unfavorable by 375, Everett was favorable by 1,410, Lake Forest Park was unfavorable by 97, Renton was favorable by 2,413, Seattle was favorable by 7,882, Shoreline was unfavorable by 299 and Tacoma was favorable by 1,258.



Transactions YTD Budget versus YTD Actual	Transactions YTD Budget versus Actual were favorable by 11,280. Three cities were favorable and four cities were unfavorable. Bellevue was unfavorable by 912, Bremerton was unfavorable by 375, Everett was favorable by 1,410, Lake Forest Park was unfavorable by 97, Renton was favorable by 2,413, Seattle was favorable by 7,882, Shoreline was unfavorable by 299 and Tacoma was favorable by 1,258.

User Account Sign-Up Metrics						
Description	Sep-18	Oct-18	Nov-18	Dec-18	Jan-19	Feb-19
Users that completed email validation	1,406	2,352	2,811	4,428	8,411	2,080
% of users that completed email validation	96%	95%	94%	91%	90%	89%
Users that completed email validation and assigned a license	823	1,515	1,358	2,205	5,468	1,412
% of users that completed email validation and assigned a license	59%	64%	48%	50%	65%	68%
Filed a Tax Return for the First Time	426	890	557	945	3,550	731

Seattle Import Account Sign-Up Metrics						
Description	Sep-18	Oct-18	Nov-18	Dec-18	Jan-19	Feb-19
Seattle Import Started	61	298	216	665	2,315	353
Seattle Import Completed	38	259	185	615	2,155	329
Seattle - % that started and completed import	62%	87%	86%	92%	93%	93%

FileLocal

Your one stop for local business licensing and tax filing

www.filelocal-wa.gov

Budget 2020-2024

March 2019

Washington Cities Business License and Tax Portal Agency
Key Assumptions for Budget
FY2020-FY2024
3/4/2019
Assumptions and Notes

Revenue

Fund Carryover	T4	Fund Carryover is the process by which unobligated funds remaining at the end of the budget period may be carried over to the next budget period. This is typically approved during the December Board Meeting
User Fees	T1	User Fees are fees charged to the business user for each city specific transaction net of zero dollar returns. The allocation methodology is based on projected transaction amounts.
Reimbursable Costs	T3	Costs to be reimbursed by participating cities.
Capital Cost Recovery Charges	T2/T4.6	Capital Cost Recovery Charge is an annual fee charged to all participating cities other than Seattle, for the purposes of reimbursing Seattle for a portion of the funding provided to pay for the start up of the Portal Agency. See Section 13.j in the Interlocal Agreement for further information.

Expense

Labor	T4.1	Labor is broken into two primary categories. Agency employees which are budgeted based on City of Seattle estimates and Incremental Labor which is based on new city additions with the calculation determined in the Interlocal Agreement.
Contracts	T4.2	Consulting and Service Fees - is comprised of Outside Accounting, State Auditor, Insurance and Bank Fees.
Overhead	T4.3	Overhead is comprised of Legal, City of Seattle Technology Fees, Office and Operating Supplies, Printing, Licenses, Travel, Marketing, Incremental
Technology Costs	T4.4	Technology Costs are outside IT Costs and comprised of ASP Hosting, Software as a Service, USPS Address Lists, Transaction Fees, IT and Security Audit, Misc. Technology, Software Development and Incremental IT.
Operating Reserve	T4.5	Operating Reserve is an unrestricted fund balance set aside to provide a cushion against unexpected events. The current operating reserve is 15% of total operating expenditures.
Incremental Labor	T4.1	Incremental Labor, Overhead and Technology Costs are amounts calculated with each new city to determine the maximum amount which costs can increase as new cities are added.
Incremental Overhead	T4.3	Incremental Labor, Overhead and Technology Costs are amounts calculated with each new city to determine the maximum amount which costs can increase as new cities are added.
Incremental Technology Cost	T4.4	Incremental Labor, Overhead and Technology Costs are amounts calculated with each new city to determine the maximum amount which costs can increase as new cities are added.

FileLocal

Your one stop for local business licensing and tax filing **www.filelocal-wa.gov**

Washington Cities Business License and Tax Portal Agency
Summary of Budget
FY2020-FY2024
3/4/2019

		Actual (A), Projection (P), Budget (B)								B/(W)						
		2018 (A)	2019 (B)	2019 (P)	2020 (B)	2021 (B)	2022 (B)	2023 (B)	2024 (B)	2019 (B) vs. 2018 (A)	2019 (P) vs. 2019 (B)	2020 (B) vs. 2019 (P)	2021 (B) vs. 2020 (B)	2022 (B) vs. 2021 (B)	2023 (B) vs. 2022 (B)	2024 (B) vs. 2023 (B)
Revenue:																
Fund Carryover	T4	-	50,000	50,000	-	-	-	-	-	50,000	-	(50,000)	-	-	-	-
User Fees	T1	212,329	328,001	319,800	395,010	488,825	610,629	637,901	668,672	115,672	(8,201)	75,210	93,815	121,804	27,273	30,771
Reimbursable Costs	T3	832,818	793,217	816,611	824,743	805,102	773,065	774,636	783,029	(39,601)	23,394	8,132	(19,641)	(32,037)	1,571	8,393
Capital Cost Recovery Charges	T2	21,000	18,000	20,000	20,000	20,000	20,000	20,000	20,000	(3,000)	2,000	-	-	-	-	-
Total Revenue B/(W)		1,066,147	1,189,218	1,206,411	1,239,753	1,313,927	1,403,694	1,432,537	1,471,701	123,071	17,193	33,342	74,173	89,767	28,843	39,164
Expenditures																
Regular Expenditures:																
Labor	T4.1	334,603	351,489	351,489	358,870	366,765	374,834	382,706	390,743	(16,886)	-	(7,381)	(7,895)	(8,069)	(7,872)	(8,037)
Contracts	T4.2	42,098	59,788	59,788	61,044	62,387	63,759	65,098	66,465	(17,690)	-	(1,256)	(1,343)	(1,373)	(1,339)	(1,367)
Overhead	T4.3	26,809	46,787	46,787	47,770	48,820	49,895	50,942	52,012	(19,978)	-	(983)	(1,051)	(1,074)	(1,048)	(1,070)
Technology Costs	T4.4	566,857	621,035	636,228	677,003	737,297	812,744	837,518	864,372	(54,178)	(15,193)	(40,775)	(60,294)	(75,447)	(24,774)	(26,854)
Operating Reserve	T4.5	-	27,094	27,094	8,677	10,806	13,118	5,473	5,822	(27,094)	-	18,417	(2,130)	(2,312)	7,645	(349)
Capital Cost Recovery Payments	T4.6	21,000	18,000	20,000	20,000	20,000	20,000	20,000	20,000	3,000	(2,000)	-	-	-	-	-
Total Regular Expenditures		991,367	1,124,193	1,141,386	1,173,363	1,246,075	1,334,350	1,361,737	1,399,414	(132,826)	(17,193)	(31,977)	(72,713)	(88,274)	(27,387)	(37,677)
Incremental Expenses from The New Partners:																
Incremental Labor	T4.1	-	46,768	46,768	47,750	48,801	49,874	50,922	51,991	(46,768)	-	(982)	(1,051)	(1,074)	(1,047)	(1,069)
Incremental Overhead	T4.3	-	7,609	7,609	7,769	7,940	8,114	8,285	8,459	(7,609)	-	(160)	(171)	(175)	(170)	(174)
Incremental Technology Cost	T4.4	-	10,648	10,648	10,872	11,111	11,355	11,594	11,837	(10,648)	-	(224)	(239)	(244)	(238)	(243)
Total Incremental Expenditures		-	65,025	65,025	66,391	67,851	69,344	70,800	72,287	(65,025)	-	(1,366)	(1,461)	(1,493)	(1,456)	(1,487)
Total Expenditures B/(W)		991,367	1,189,218	1,206,411	1,239,753	1,313,927	1,403,694	1,432,537	1,471,701	(197,851)	(17,193)	(33,342)	(74,173)	(89,767)	(28,843)	(39,164)
Excess (Deficit)		74,780	-	-	-	-	-	-	-	(74,780)	-	-	-	-	0	(0)

Revenue

T4 FY19 Fund Carryover is $50k. This is primarily related to ADA Compliance work that originated out of the ADA Audit. No fund carryover is projected for FY20.

T1 User Fees in FY20 are up BY $75K comparing to FY19(P). This is due to an increase in transaction count by approximately 25K.

T3 FY20 Reimbursable Costs is approximately $8K higher than FY19(P). This is primarily related to the increase in user fees that are offset against fund carryover.

Expense

T4.1 **FY18 Labor is favorable by $20.5k compared to FY19. This is primarily due to admin position not filled for 6 months in FY18. Final labor costs to be updated. Note: Labor to be updated**

T4.2 FY20 Contracts slightly increase due to the estimated inflation adjustments.

T4.3 No additional participating cities are projected for FY20. FY20 Overhead slightly increase due to the stimated inflation adjustments.

T4.4 FY20 Technology costs are up $41K. This is primarily due to the increase in transaction count, approximately 25K more counts.
Please note there is a reclass ADA compliance costs from Software Development to Misc. Technology Expense for the breakdown of technology costs at [Expense] tab.
As a result, $50K is removed out of Software Development while $30K is added to Misc. Technology Expense in FY20.

T4.1/.3/.4 No additional participating cities are projected for FY20 and thus, there are slight increase in incremental labor, overhead and techonology costs.

T4.5 Operating Reserve in FY20 decrease by approximately $18K, primarily due to the accumulated operating reserves in previous years.

FileLocal

Budget 2020-2024

Your one stop for local business licensing and tax filing

www.filelocal-wa.gov

3. Schedule of Estimated Transaction Count

	Transaction Count							
	2018 (A)	2019 (B)	2019 (P)	2020 (B)	2021 (B)	2022 (B)	2023 (B)	2024 (B)
T1. Transaction Count								
Bellevue	16,118	22,800	21,000	23,100	25,410	27,951	30,746	33,821
Bremerton	571	1,568	500	600	720	864	1,037	1,244
Everett	5,062	6,937	8,000	8,800	9,680	10,648	11,713	12,884
Lake Forest Park	426	1,260	650	780	936	1,123	1,348	1,617
Renton	-	1,541	5,000	7,000	8,400	10,080	12,096	14,515
Seattle	29,932	40,475	51,000	68,850	92,948	125,479	125,479	125,479
Shoreline	1	1,890	450	540	648	778	933	1,120
Tacoma	13,649	20,000	20,000	22,000	24,200	26,620	29,282	32,210
Total	65,759	96,471	106,600	131,670	162,942	203,543	212,634	222,891

	Actual (A), Projection (P), Budget (B) - B/(W)						
	2019 (B) vs. 2018 (A)	2019 (P) vs. 2019 (B)	2020 (B) vs. 2019 (P)	2021 (B) vs. 2020 (B)	2022 (B) vs. 2021 (B)	2023 (B) vs. 2022 (B)	2024 (B) vs. 2023 (B)
T1. Transaction Count							
Bellevue	6,682	(1,800)	2,100	2,310	2,541	2,795	3,075
Bremerton	997	(1,068)	100	120	144	173	207
Everett	1,875	1,063	800	880	968	1,065	1,171
Lake Forest Park	834	(610)	130	156	187	225	270
Renton	1,541	3,459	2,000	1,400	1,680	2,016	2,419
Seattle	10,543	10,525	17,850	24,098	32,532	-	-
Shoreline	1,889	(1,440)	90	108	130	156	187
Tacoma	6,351	-	2,000	2,200	2,420	2,662	2,928
Total	30,712	10,129	25,070	31,272	40,601	9,091	10,257

4. Schedule of Estimated User Fee Revenue and Expenses

	All Years	User & Transaction Fees							
	% of $0 Filers	2018 (A)	2019 (B)	2019 (P)	2020 (B)	2021 (B)	2022 (B)	2023 (B)	2024 (B)
T1. User Fee Revenue									
Bellevue	25%	$ 52,043	$ 77,520	$ 63,000	$ 69,300	$ 76,230	$ 83,853	$ 92,238	$ 101,462
Bremerton	25%	$ -	$ 5,331	$ 1,500	$ 1,800	$ 2,160	$ 2,592	$ 3,110	$ 3,732
Everett	25%	$ 16,345	$ 23,586	$ 24,000	$ 26,400	$ 29,040	$ 31,944	$ 35,138	$ 38,652
Lake Forest Park	25%	$ 1,376	$ 4,284	$ 1,950	$ 2,340	$ 2,808	$ 3,370	$ 4,044	$ 4,852
Renton	25%	$ 1,844	$ 5,239	$ 15,000	$ 21,000	$ 25,200	$ 30,240	$ 36,288	$ 43,546
Seattle	25%	$ 96,647	$ 137,615	$ 153,000	$ 206,550	$ 278,843	$ 376,437	$ 376,437	$ 376,437
Shoreline	25%	$ 3	$ 6,426	$ 1,350	$ 1,620	$ 1,944	$ 2,333	$ 2,799	$ 3,359
Tacoma	25%	$ 44,071	$ 68,000	$ 60,000	$ 66,000	$ 72,600	$ 79,860	$ 87,846	$ 96,631
Total		$ 212,329	$ 328,001	$ 319,800	$ 395,010	$ 488,825	$ 610,629	$ 637,901	$ 668,672
User Fee Expenses									
Bellevue	0%	$ 23,123	$ 34,200	$ 31,500	$ 36,960	$ 40,656	$ 44,722	$ 49,194	$ 54,113
Bremerton	0%	$ -	$ 2,352	$ 750	$ 960	$ 1,152	$ 1,382	$ 1,659	$ 1,991
Everett	0%	$ 7,262	$ 10,406	$ 12,000	$ 14,080	$ 15,488	$ 17,037	$ 18,740	$ 20,615
Lake Forest Park	0%	$ 611	$ 1,890	$ 975	$ 1,248	$ 1,498	$ 1,797	$ 2,157	$ 2,588
Renton	0%	$ 819	$ 2,312	$ 7,500	$ 11,200	$ 13,440	$ 16,128	$ 19,354	$ 23,224
Seattle	0%	$ 42,941	$ 60,713	$ 76,500	$ 110,160	$ 148,716	$ 200,767	$ 200,767	$ 200,767
Shoreline	0%	$ 1	$ 2,835	$ 675	$ 864	$ 1,037	$ 1,244	$ 1,493	$ 1,792
Tacoma	0%	$ 19,581	$ 30,000	$ 30,000	$ 35,200	$ 38,720	$ 42,592	$ 46,851	$ 51,536
Total		$ 94,340	$ 144,707	$ 159,900	$ 210,672	$ 260,706	$ 325,669	$ 340,214	$ 356,625

	Actual (A), Projection (P), Budget (B)						
	2019 (B) vs. 2018 (A)	2019 (P) vs. 2019 (B)	2020 (B) vs. 2019 (P)	2021 (B) vs. 2020 (B)	2022 (B) vs. 2021 (B)	2023 (B) vs. 2022 (B)	2024 (B) vs. 2023 (B)
T1. User Fee Revenue							
Bellevue	$ 25,477	$ (14,520)	$ 6,300	$ 6,930	$ 7,623	$ 8,385	$ 9,224
Bremerton	$ 5,331	$ (3,831)	$ 300	$ 360	$ 432	$ 518	$ 622
Everett	$ 7,241	$ 414	$ 2,400	$ 2,640	$ 2,904	$ 3,194	$ 3,514
Lake Forest Park	$ 2,908	$ (2,334)	$ 390	$ 468	$ 562	$ 674	$ 809
Renton	$ 3,396	$ 9,761	$ 6,000	$ 4,200	$ 5,040	$ 6,048	$ 7,258
Seattle	$ 40,968	$ 15,385	$ 53,550	$ 72,293	$ 97,595	$ -	$ -
Shoreline	$ 6,423	$ (5,076)	$ 270	$ 324	$ 389	$ 467	$ 560
Tacoma	$ 23,929	$ (8,000)	$ 6,000	$ 6,600	$ 7,260	$ 7,986	$ 8,785
Total	$ 115,672	$ (8,201)	$ 75,210	$ 93,815	$ 121,804	$ 27,273	$ 30,771
User Fee Expenses							
Bellevue	$ (11,077)	$ 2,700	$ (5,460)	$ (3,696)	$ (4,066)	$ (4,472)	$ (4,919)
Bremerton	$ (2,352)	$ 1,602	$ (210)	$ (192)	$ (230)	$ (276)	$ (332)
Everett	$ (3,143)	$ (1,595)	$ (2,080)	$ (1,408)	$ (1,549)	$ (1,704)	$ (1,874)
Lake Forest Park	$ (1,279)	$ 915	$ (273)	$ (250)	$ (300)	$ (359)	$ (431)
Renton	$ (1,492)	$ (5,189)	$ (3,700)	$ (2,240)	$ (2,688)	$ (3,226)	$ (3,871)
Seattle	$ (17,771)	$ (15,788)	$ (33,660)	$ (38,556)	$ (52,051)	$ -	$ -
Shoreline	$ (2,834)	$ 2,160	$ (189)	$ (173)	$ (207)	$ (249)	$ (299)
Tacoma	$ (10,419)	$ -	$ (5,200)	$ (3,520)	$ (3,872)	$ (4,259)	$ (4,685)
Total	$ (50,367)	$ (15,194)	$ (50,772)	$ (50,034)	$ (64,962)	$ (14,545)	$ (16,411)

FileLocal

Budget 2020-2024

Your one stop for local business licensing and tax filing

www.filelocal-wa.gov

	Reimbursable Costs								Actual (A), Projection (P), Budget (B)						
	2018 (A)	2019 (B)	2019 (P)	2020 (B)	2021 (B)	2022 (B)	2023 (B)	2024 (B)	2019 (B) vs. 2018 (A)	2019 (P) vs. 2019 (B)	2020 (B) vs. 2019 (P)	2021 (B) vs. 2020 (B)	2022 (B) vs. 2021 (B)	2023 (B) vs. 2022 (B)	2024 (B) vs. 2023 (B)
T3. Reimbursement	$ 832,818	$ 793,217	$ 816,611	$ 824,743	$ 805,102	$ 773,065	$ 774,636	$ 783,029							
Bellevue	$ 79,125	$ 70,517	$ 72,597	$ 73,320	$ 71,574	$ 68,725	$ 68,865	$ 69,611	8,608	(2,080)	(723)	1,746	2,848	(140)	(746)
Bremerton	$ 11,854	$ 36,091	$ 37,156	$ 37,526	$ 36,632	$ 35,174	$ 35,246	$ 35,628	(24,237)	(1,064)	(370)	894	1,458	(71)	(382)
Everett	$ 36,821	$ 32,760	$ 33,726	$ 34,062	$ 33,251	$ 31,928	$ 31,992	$ 32,339	4,061	(966)	(336)	811	1,323	(65)	(347)
Lake Forest Park	$ 8,955	$ 7,932	$ 8,166	$ 8,247	$ 8,051	$ 7,731	$ 7,746	$ 7,830	1,023	(234)	(81)	196	320	(16)	(84)
Renton	$ 19,117	$ 35,060	$ 36,094	$ 36,454	$ 35,586	$ 34,169	$ 34,239	$ 34,610	(15,943)	(1,034)	(359)	868	1,416	(69)	(371)
Seattle	$ 543,559	$ 483,703	$ 497,969	$ 502,928	$ 490,951	$ 471,415	$ 472,373	$ 477,491	59,856	(14,266)	(4,959)	11,977	19,536	(958)	(5,118)
Shoreline	$ 5,465	$ 13,326	$ 13,719	$ 13,856	$ 13,526	$ 12,987	$ 13,014	$ 13,155	(7,861)	(393)	(137)	330	538	(26)	(141)
Tacoma	$ 127,922	$ 113,827	$ 117,184	$ 118,351	$ 115,532	$ 110,935	$ 111,160	$ 112,365	14,095	(3,357)	(1,167)	2,819	4,597	(225)	(1,204)
Total	$ 832,818	$ 793,217	$ 816,611	$ 824,743	$ 805,102	$ 773,065	$ 774,636	$ 783,029	39,601	(23,394)	(8,132)	19,641	32,037	(1,571)	(8,393)

FileLocal

Your one stop for local business licensing and tax filing

www.filelocal-wa.gov

State Audit

March 2019

Audit Overview and Timing

Audit Scope

State Auditors Office has identified the following areas for audit.

- Open Public Meeting Act
- Financial condition and fiscal sustainability
- Third-party cash receipting

Timeline

- End of April

Americans With Disabilities Act (ADA) Audit Update

March 2019

- **July 2018**
  - Audit completed
  - FileLocal Website was found to be partially compliant
- **December 2018**
  - Avenu and the Agency, reviewed and prioritized findings.
  - Avenu and the Agency agreed that Avenu will absorb the cost for ADA compliance items.
- **January 2019**
  - Tacoma meeting to review findings and proposed prioritization.
  - Tacoma agreed with the development methodology.
- **March 2019**
  - Q1’19 Release updated to ensure all instances of the alternative text for image links is informative. This audit finding was closed (see page 4).
  - Q2’19 release ADA development work agreed to.

FileLocal ADA Enhancements

Q1, 2019.1

GM-1950 – Ensure alternative text for image links is informative

Vendor description:

[Issue]
The FileLocal image link has an alt value, but the target anchor needs to be communicated with the alt value.
The "Your one stop for local business licensing and tax filing" link lacks a target anchor in the alt value.
[Impact]
Screen reader users use the alt attribute to understand the purpose of the image link. When that information is not available, the users may follow the link and go to unintended places.

Avenu Solution:

For the example above, text was added to the alt value to read, “FileLocal Home Page.” The work in this task covered hyperlinks represented by images. There are three types of images in this category:

- Navigational images – for example, buttons. The alt text will now reflect the label of the button.
- Hyperlink images – using the text attribute for alternate text, the text will now concisely describe where the link directs to.
- Image controls – a simple picture on the page. The Alt text will state what the image is. For example, the image displaying (“Your one stop shop for…”) will say that. The UBI code diagram will state "UBI Code Diagram.”

Pages Impacted:

The FileLocal Portal does not use many image links. For this exercise, image links were identified and revised on the following pages:

- rtnSetup.aspx
- Search.aspx
- Users.aspx
- Header.ascx
- Footer.ascx
- LicenseQuestionAnswer.ascx
- DataImport.aspx
- TaxpayerSignup.aspx
- UbiQuestion.aspx
- Default_FileLocal.aspx

Violations by Avenu Phase

Description	Media Type	Occurrence Rate	Severity	Noticeability	Tractability	Priority	Avenu Phase	Release	Projected Release
Ensure alternative text for image links is informative	Links	96%	8	7	2	10	1	Q1'19	
Provide alternative text for images	Images	4%	10	10	2	9.1	1		Q2'19
Ensure images provide informative alternative text	Images	4%	10	7	1	8.5	1		Q2'19
Ensure a valid skip link target is present and is located appropriately	Navigation	50%	8	5	4	6.7	1		Q2'19
Ensure color is not used as the sole method of indicating selection	Color and Contrast	29%	6	2	6	2.8	1		Q2'19
Provide a valid label for form fields	Forms	29%	10	6	2	8.5	2		
Ensure dialogs use proper structure	Dialogs	4%	8	8	3	6.7	2		
Ensure link text is meaningful within context	Links	8%	6	6	2	5.4	2		
Ensure form field labels are unique	Forms	13%	7	5	6	3.9	2		
Ensure custom controls provide proper textual name, role, and state information	Custom Controls	8%	7	4	5	3.9	2		
Ensure error messages are explicitly indicated at the beginning of a form after submit	Forms	21%	6	3	5	3.4	2		
Ensure headers and cells are properly associated	Data Tables	33%	10	7	4	8	3		
Ensure color is not the sole means of communicating information	Color and Contrast	29%	10	2	5	5.7	3		
Provide an accessible alert method for content changes that occur without explicit user knowledge	ARIA and Dynamic Content	4%	8	7	7	4.4	3		
Ensure color is not the sole means of indicating error messages	Color and Contrast	42%	10	6	5	7.5	4		
Ensure keyboard focus is indicated visually	Focus Control	75%	7	5	5	6.5	4		
Ensure form field constraints are clearly indicated	Forms	42%	7	3	6	4.2	4		
Avoid using event handlers that trigger focus or context changes on user input	Focus Control	17%	8	5	6	4.6	5		
Ensure all active elements receive keyboard focus	Keyboard Accessibility	4%	8	4	7	3.3	5		
Provide fieldsets for groups of form controls	Forms	21%	6	4	6	3.2	5		
Provide a clear indication of fields in error for information that is submitted	Forms	4%	6	4	6	2.6	5		
Ensure implicit list markup is avoided	Lists	4%	6	3	7	1.8	5		
Avoid the sole use of device-dependent event handlers	Keyboard Accessibility	50%	8	7	2	8.4	6		
Ensure CSS background images that convey meaning have textual and visible equivalents	Images	17%	8	7	2	7.3	TBD		

FileLocal

Your one stop for local business licensing and tax filing

www.filelocal-wa.gov

New City Update

March 2019

Scheduled

City	Launch	Type	Notes
Shoreline	2019.1	Subscriber City	City launched in early January and is fully functional, with 154 transactions being process in January and February.
Bremerton	2019.1	Subscriber City	City launched in mid-March and is fully functional.

Prospects

City	Launch	Type	Notes
Vision Software	N/A	N/A	The Agency was notified in February 2019 that the company will not be developing an interface with FileLocal in Q2'19. Unless an a City makes this a condition for utilizing Vision's backend, it is unlikely that Vision will be pursuing this further.
Kent	2019.3	TBD	City is developing a SOR. Once this is complete, the agency will work with the city to schedule a date for FileLocal Implementation.
Snoqualmie	2020.2	Principal City	City is reviewing various back-end solutions
Des Moines	TBD	TBD	City is reviewing various back-end solutions.
Issaquah	TBD	Principal City	City is reviewing various back-end solutions.
Various	N/A	TBD	Various cities have reached out to FileLocal.

Filelocal
Vendor Contact List
March 5, 2019

Vendor
Ad Specialties & Promotions
Associated Recreational Council
Association of Washington Cities
Bellevue Vendor
Blue Soda Promo
City of Bremerton Tax & License
City of Everett Tax & License
City of Seattle Capital Recovery
City of Seattle Tax & License
City of Seattle Treasury Dept
City of Tacoma Tax & License
Department of Information Technology
Dynamic Language
e.Gov Systems
Everett Vendor
Foster Pepper
Francis & Company
Getty Images
Greg Kauper
Ingallina's Box Lunch
Jamie Carnell
Keeney's
Kenyon Disend
Kevin Fitzpatrick
Kubra
Laurie McVay
Level Access
Leviathan
Overnight Printing & Graphics
Performance Dimensions Group
Seattle Dept of Information Tech
Seattle Finance and Adm
Secretary of State
State of Washington-Consolidated Tech
Tacoma Vendor
Vision Municipal Solutions
WAPRO
Washington Cities Insurance Authority
Washington Finance Officers Association
Washington State Auditor's Office
Wells Fargo
Wendy Thomaston
WFOA Conference