RESOLUTION NO. 2016-04

A Resolution of the Washington Multi-City Business License and Tax Portal Agency Executive Board adopting Information Technology Security Policies

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

Whereas, the Program Manager, working with a City of Seattle information technology contracted security firm, has developed Information Technology Security Policies, as set forth in Attachment A, in accordance with the Section 4.a.v. of the Agreement ("Guiding Principles and Goals – Security"), which seeks to safeguard taxpayer, licensee and particitating City data;

Whereas, the Agreement specifies that the Operations Committee shall assist in the review of the Operations Policies and amendments thereto;

Whereas, Operations Policies will be developed over time and subject to amendments, and;

Whereas, approval of Operations Policies requires a supermajority 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 adopts the Information Technology Security Policies set forth in Attachment A to this resolution, which shall hereafter constitute a new "Security Policies" chapter of the Operations Policies and Procedures manual of the Portal Agency.

ADOPTED this _____ day of _____, 2016.

ATTEST:

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

_____
Board Secretary

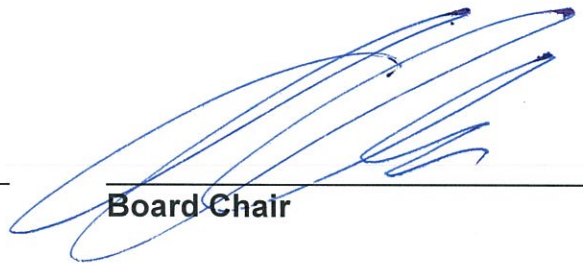
_____
Board Chair

SECTION 1. The Executive Board hereby adopts the Information Technology Security Policies set forth in Attachment A to this resolution, which shall hereafter constitute a new "Security Policies" chapter of the Operations Policies and Procedures manual of the Portal Agency.

ADOPTED this _____ day of _____, 2016.

ATTEST:

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



Board Secretary

Board Chair



Information Technology Securities Policy Manual

TABLE OF CONTENTS

POL-001: Information Management 2
POL-010: Information Classification 6
POL-020: Access Control 10
POL-030: Encryption 14
POL-040: Infrastructure 17
POL-050: Physical and Environmental 22
POL-060: Third Party Management and Outsourced Services 26
POL-070: Data Backup 31
POL-080: Data Storage Media Library Management 34
POL-090: Compliance 37
POL-100: Incident Response 41
POL-110: Security Risk Assessment 46
POL-130: System Development Life Cycle 48
POL-140: Business Continuity 51
GDE-200: Guidelines for Information Owners and Custodians 54

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

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 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. 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:

- 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 CISO, 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 CISO, or designee.
- Assisting the CISO, or 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 CISO, 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 CISO, or designee, and to a City's CISO, or designee.



- Assisting the FileLocal CISO, 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 27002:2005:

- Section 4.1 – Assessing Security Risks
- Section 7.1.1 – Inventory of Assets
- Section 7.1.2 – Ownership of Assets
- Section 7.2.1 – Classification Guidelines
- Section 7.2.2 – Information Labeling and Handling
- Section 10.7.2 – Disposal of Media
- Section 10.7.3 – Information Handling Procedures
- Section 10.8.3 – Physical Media in Transit
- Section 10.8.4 – Electronic Messaging
- Section 12.3 – Cryptographic Controls
- Section 15.1 – Compliance with Legal Requirements

7. Related Documents

- Information and Media Handling Standard
- Information Retention Standard

ACCESS CONTROL

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 Executive with Information Security responsibilities.

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

H. User access activities shall be continuously monitored and verified regularly to detect unauthorized access in a timely manner.

I. 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. 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 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 CISO, OR 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 breaches, and reporting them to FileLocal and the CISO, or designee.
- Assisting the CISO, or 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 the CISO, or 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 and a City's CISO, or designee.
- Assisting the FileLocal CISO, or 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 and a City's CISO, or 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 27002:2005:

- Section 6.1.3 – Allocation of Information Security Responsibilities
- Section 8.2.1 – Management Responsibilities
- Section 10.1.3 – Segregation of Duties
- Section 11 – Access Control

7. Related Documents

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

ENCRYPTION

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 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. FileLocal Executive with Information Security responsibilities 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 Executive with Information Security Responsibilities.

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 27002:2005:

- Section 10.5.1 – Information Back-up
- Section 10.6.2 – Security of Network Services
- Section 10.8.1 – Information Exchange Policies and Procedures
- Section 10.9.1 – Electronic Commerce
- Section 10.9.2 – Online Transactions
- Section 11.5.3 – Password Management System
- Section 12.3 – Cryptographic Controls
- Section 15.1.6 – Regulation of Cryptographic Controls
- Section 11.4.2 – User Authentication for External Connections
- Section 12.2.3 – Message integrity

7. Related Documents

- Encryption Standard

INFRASTRUCTURE

1. INTRODUCTION

The following policies and subsequent standards are expressly authored as foundation documents to manage the Washington Multi-City Business License and Tax Portal agency (FileLocal) infrastructure. In the marketplace reality, such as with intrusion, unwarranted access, and attacks, FileLocal must make its infrastructure safe, to protect its assets, staff and intellectual property. 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 the corporate 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 governing principles on the security of its infrastructure. Such expression of artifacts is intended to ensure that FileLocal 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:

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

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 has signed a risk acceptance form. The Risk Acceptance Form shall be authenticated by the Executive with Information Security responsibilities.

4. POLICY STATEMENTS

A. FileLocal seeks to ensure its infrastructure (managed by vendors and the City of Seattle (for FileLocal Agency staff per Loaned Staff Agreement adopted in 2013) is properly used, prevents unauthorized access or use, maintains availability and protects the security of information resources.

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

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

D. FileLocal seeks to ensure a formal risk assessment is performed on the infrastructure at least once a year by vendors and participating cities CISO, or designee, offices. The risk assessment shall identify / confirm key risks imposed on the infrastructure and determine the security controls required to mitigate those risks within acceptable limits.

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

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

G. All security events shall be continuously monitored.

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

I. File Local seeks to ensure vendors supply the Agency equipment that is maintained in accordance with the supplier's recommended service intervals and specifications.

5. ROLES AND RESPONSIBILITIES

A. FileLocal Executive with Information Security responsibilities

Executive with Information Security responsibilities is responsible for:

- Developing and implementing strategies to ensure users are aware of using security policies, procedures and benefits.
- Working with vendors and participating cities to perform organizational self-assessment periodically to ensure compliance with this policy and related artifacts.
- Working with vendors and participating cities to 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 security policies and standards.
- Reviewing any architectural initiative(s) to determine compliance with FileLocal security policies and standards.

- Working with vendors and participating cities to lead any investigation of any reported security breaches in FileLocal systems, business applications or networks.
- Communicating with vendors and participating cities the importance of properly authorizing inbound and outbound traffic through the firewall - as needed by the business.

B. FileLocal Agency Staff

FileLocal is responsible for:

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

C. Vendors

Vendors are responsible for:

- Assisting FileLocal to implement and maintain security controls mandated by this policy and related artifacts.
- Providing assistance to the FileLocal 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 standards and procedures.
- Assisting Participating Cities 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.
- Reviewing the configuration of infrastructure components on a regular basis.
- Identifying any non-compliant computational activities, and report such to FileLocal and the Executive with Information Security responsibilities.
- Recording security incidents relating to the infrastructure, report them to the Executive with Information Security responsibilities.



- Providing assistance to the CISO, or designee, for investigations of security breaches in regards to the infrastructure.
- Providing periodic reports to FileLocal and the Executive with Information Security responsibilities.

D. Participating Cities

Participating Cities are responsible for:

- Accessing only those FileLocal information resources to which they have been granted permission.
- Accessing FileLocal 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 or that the use of computational resources is in compliance with a City's CISO, or designee, policies and standards.
- Immediately reporting violations of this policy and related standards to FileLocal Help Desk.
- Working within and respecting the intention / purpose /objectives of this policy and related artifacts.
- Not allowing unapproved changes or system alterations and application security configuration of their computers/devices.
- Protecting FileLocal, City and FileLocal 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 27002:2005:

- Section 7.1 – Responsibility for assets
- Section 9.1 – Secure areas
- Section 9.2 – Equipment security
- Section 10.1 – Operational procedures and responsibilities
- Section 10.2 – Third party service delivery management
- Section 10.3 – System planning and acceptance
- Section 10.5 – Back-up
- Section 10.6 – Network security management
- Section 10.10 – Monitoring
- Section 11.4 – Network access control

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

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

D. FileLocal shall apply strong physical controls around handling visitors that access FileLocal facilities.

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

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

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

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

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

J. 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.

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

L. Doors and windows of restricted areas shall be locked when unattended, and external protection shall be considered for windows on the ground floor.

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

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 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 Policy uses and assimilates the following bodies of recognized knowledge:

ISO 27002:2005:

- Section 4.1 – Assessing Security Risks
- Section 4.2 – Treating Security Risks
- Section 9.1.1 – Physical security perimeter
- Section 9.1.2 – Physical entry controls
- Section 9.1.3 – Securing offices, rooms, and facilities
- Section 9.1.4 – Protecting against external and environmental threats
- Section 9.1.5 – Working in secure areas
- Section 9.2.1 – Equipment sitting and protection
- Section 9.2.3 – Cabling security
- Section 9.2.7 – Removal of property
- Section 11.3.3 – Clear Desk and Clear Screen Policy

7. Related Documents

- Physical and Environmental Standard

THIRD PARTY MANAGEMENT AND OUTSOURCED SERVICES

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 the Washington Multi-City Business License and Tax Portal Agency (FileLocal) 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
- Vendors
- Consultants
- Participating cities
- All business partners and parties

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 equivalent employees, who are obligated under, emails and memos, forms of contracts, blanket agreements, and other such contracts.
- 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 FileLocal has signed a risk acceptance form. The Risk Acceptance Form shall be authenticated by the Executive with Information Security responsibilities.

4. POLICY STATEMENTS

A. IT services shall be obtained from service providers that are capable of providing effective security controls.

B. Third party access and outsourced services shall be supported by documented contracts and/or service level agreements. These agreements shall:

C. Define the security service level commitments by the IT service provider and each Third Party.

D. Identify responsibilities for all parties involved, including responsibilities with respect to legal matters.

E. Mandate each Third Party's compliance with FileLocal Information Management Policies and Standards.

F. Promote compliance with applicable governance, legal and regulatory requirements.

G. Govern the cooperation on investigation efforts of security incidents.

H. FileLocal shall require approval to the use of a third parties computational resources in advance of remote or internal access to FileLocal computational resources.

I. 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 on business requirements.

J. No Third Party connection shall be authorized to connect to or use the FileLocal service without providing evidence to FileLocal that the Third Party has completed an assessment and acceptance of the risk to the shared infrastructure.

K. Third Parties shall access FileLocal computational resources using hardware, software and network components as per agreement.

L. 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.

M. FileLocal shall monitor the security of service provided by each Third Party to ensure compliance with the contracted SLA.

N. Any change in Third Party's access shall follow FileLocal Change Management Process.



O. FileLocal shall have the right to audit the security measures at each Third Party and third party devices accessing FileLocal computational resources, or be provided with the most recent external audit of Third Party's information system (e.g. CICA Section 5970, SAS70) related to the service being provided to ensure compliance with the agreement.

P. Each Third Party connection shall be reviewed regularly to confirm a continuing business need.

Q. 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.

R. Third Parties shall receive appropriate training and regular updates in FileLocal' 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.

S. Third Party agents working in secure areas shall be supervised at all times to prevent opportunities for malicious activities.

T. Non-disclosure agreements should be signed where appropriate.

5. ROLES AND RESPONSIBILITIES

A. 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.
- 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.

B. 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.

C. Vendors

Vendors are responsible for:



- Ensuring that Third Parties working with FileLocal information resources follow this policy.
- 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.
- Identifying access control breaches, and reporting them to FileLocal 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.

D. Participating Cities

Participating Cities are responsible for:

- Promptly reporting violations of this policy and related standards to Help Desk and to a City's CISO, or designee.

6. COMPLIANCE

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

ISO 27002:2005:

- Section 4.1 – Assessing Security Risks
- Section 4.2 – Treating Security Risks
- Section 6.1.5 – Confidentiality agreements
- Section 6.2.1 – Identification of risks related to external parties
- Section 6.2.3 – Addressing security in third party agreements
- Section 8.2.2 – Information security awareness, education, and training
- Section 9.1.2 – Physical entry controls
- Section 10.10.1 – Audit logging
- Section 10.10.2 – Monitoring system use
- Section 11.1 – Business Requirement for Access Control
- Section 11.2 – User Access Management
- Section 11.4.2 – User authentication for external connections
- Section 11.5.2 – User identification and authentication
- Section 11.6 – Application and Information Access Control

7. PURPOSE

- 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

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

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 Executive with Information Security responsibilities.

4. POLICY STATEMENTS

A. FileLocal shall adopt formal procedures for the management, handling, and storage of removable data storage media (for example, tapes, disks, and cassettes).

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

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

D. If no longer required, the previous contents of any re-usable media to be removed from FileLocal shall be sanitized.

E. 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.

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

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

H. 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.

I. FileLocal shall control access to removable data storage media in accordance Access Control Policy and related Standards.

5. Roles and Responsibilities

A. 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 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 uses and assimilates the following bodies of recognized knowledge:

ISO 27002:2005:

- Section 7.1.1 – Inventory of assets
- Section 7.1.2 – Ownership of assets
- Section 7.2.2 – Information labelling and handling
- Section 9.2.7 – Removal of property
- Section 10.7.1 – Management of removable media
- Section 10.7.2 – Disposal of media
- Section 10.7.3 – Information handling procedures
- Section 10.10.1 – Audit logging
- Section 11.2 – 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

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 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 Executive with Information Security responsibilities.

D. FileLocal supports a 'Whistle Blower' arrangement where the Executive with Information Security responsibilities 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. Executive with Information Security responsibilities

Executive with Information Security responsibilities 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 are 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 27002:2005:

- Section 4.1 – 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
- Section 13.1.1 – Reporting information security events
- Section 13.2.1 – Responsibilities and procedures
- Section 13.2.2 – Learning from information security incidents
- Section 13.2.3 – Collection of evidence

7. RELATED DOCUMENTS

- Incident Response Standard

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)

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 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. Executive with Information Security responsibilities

Executive with Information Security responsibilities 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 Data Backup Policy uses and assimilates the following bodies of recognized knowledge:

ISO 27002:2005:

- Section 12.2 – Correct Processing in Applications
- Section 12.4 – Security of System Files
- Section 12.5 – Security in Development and Support Processes

7. Related Documents

- Secure Application Development Standard
- Software Acquisition, Certification, and Accreditation Standard

BUSINESS CONTINUITY

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 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. Executive with Information Security responsibilities

Executive with Information Security responsibilities 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 are 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 Data Backup Policy uses and assimilates the following bodies of recognized knowledge:

ISO 27002:2005:

- Section 14 – Business Continuity Management

7. RELATED DOCUMENTS

- N/A

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

D. Storage Media Disposal

Data Storage Media Disposal is the process of eliminating information assets from removable media that is no longer required. Deleting 'RESTRICTED' and 'CONFIDENTIAL' information stored on removable 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.

3. 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

4. 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

5. 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

6. 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

7. 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

8. 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

9. 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.