

CITY OF SPOKANE ADMINISTRATIVE POLICY	ADMIN 5300-17-06 LGL 2017-0030
TITLE: Information Security EFFECTIVE DATE: July 11, 2017 REVISION EFFECTIVE DATE: December 15, 2017	

1.0 GENERAL

- 1.1 This policy is based upon ISO/IEC 27002:2013(E) and is structured to include the 19 main security category areas within the standard.

This policy is a high level policy which is supplemented by additional security policy documents which provide detailed policies and guidelines relating to specific security controls.

- 1.2 Information is an asset that the organization has a duty and responsibility to protect. The availability of complete and accurate information is essential to the organization functioning in an efficient manner, and to providing products and services to our community.

The purpose and objective of this Information Security Policy is to set out a framework for the protection of the City of Spokane's information assets:

- 1.2.1 To protect the city's information from all threats, whether internal or external, deliberate or accidental
 - 1.2.2 To enable secure information sharing
 - 1.2.3 To encourage consistent and professional use of information
 - 1.2.4 To ensure that users are clear about their roles in using and protecting information
 - 1.2.5 To ensure business continuity and minimize business damage
 - 1.2.6 To protect the City of Spokane from legal liability and the inappropriate use of information.
- 1.3 This document and the information security policies adopted by the City of Spokane hereunder (collectively, the "Information Security Management System") define the principles and terms of City of Spokane's Information Security Management Program (the "Information Security Program") and the responsibilities of the members of the City of Spokane community in carrying out the Information Security Program.

The information resources included in the scope of the Information Security Policies are:

- 1.3.1 All data, regardless of the storage medium (e.g., paper, cloud based, electronic tape, cartridge, disk, CD, DVD, external drive, copier hard drive, etc.) and regardless of form (e.g., text, graphic, video, audio, etc.).
- 1.3.2 The computing hardware and software Systems that process, transmit and store data; and
- 1.3.3 The Networks (as defined in Section IV below) that transport data.

The Information Security Management System are City of Spokane-wide policies that apply to all individuals who access, use or control Information Resources at the City of Spokane, including staff, temporary staff, seasonal staff, as well as contractors, consultants and other agents of the City of Spokane and/or individuals authorized to access Information Resources by affiliated company or organization.

1.4 TABLE OF CONTENTS

- 1.0 GENERAL
- 2.0 DEPARTMENTS/DIVISIONS AFFECTED
- 3.0 REFERENCES
- 4.0 DEFINITIONS
- 5.0 POLICY
- 6.0 RESPONSIBILITIES
- 7.0 APPENDICES

2.0 DEPARTMENTS/DIVISIONS AFFECTED

Applicable to all departments and divisions.

3.0 REFERENCES

City of Spokane Policies and Procedures (See Appendices)

ISO27001 Sections: 5.1.a and A.4.2

ISO/IEC 27002:2013(E)

PCI-DSS Section: 12.1

RCW 42.56.420c

Spokane Municipal Code (See Appendices)

4.0 DEFINITIONS

- 4.1 "Asset" means anything that has value to the organization.
- 4.2 "Control" is defined as managing risk, including policies, procedures, guidelines, practices.
- 4.3 "Guideline" is a description that clarifies what should be done and how.
- 4.4 "Information Security" means Information Security Preservation of confidentiality, integrity and availability of information.
- 4.5 "Policy" is the overall intention and direction as formally expressed by management.
- 4.6 "Risk" is the combination of the probability of an event and its consequences.
- 4.7 "Third Party" is when a person or body that is recognized as being independent.
- 4.8 "Threat Potential" is the cause of an unwanted incident, which may result in harm to a system.
- 4.9 "Vulnerability" is the weakness of an asset that can be exploited by one or more threats.
- 4.10 "Network" means the electronic information resources that are implemented to permit the transport of data between interconnected endpoints. Network components may include routers, switches, hubs, cabling, telecommunications, VPNs and wireless access points.
- 4.11 "ISO" is defined as Information Security Officer.
- 4.12 "CITO" is defined as Chief Innovation Technology Officer.

5.0 POLICY

5.1 The Information Security Policy is a high level document, and adopts a number of controls to protect information. The controls are delivered by policies, standards, processes, procedures, supported by training and tools.

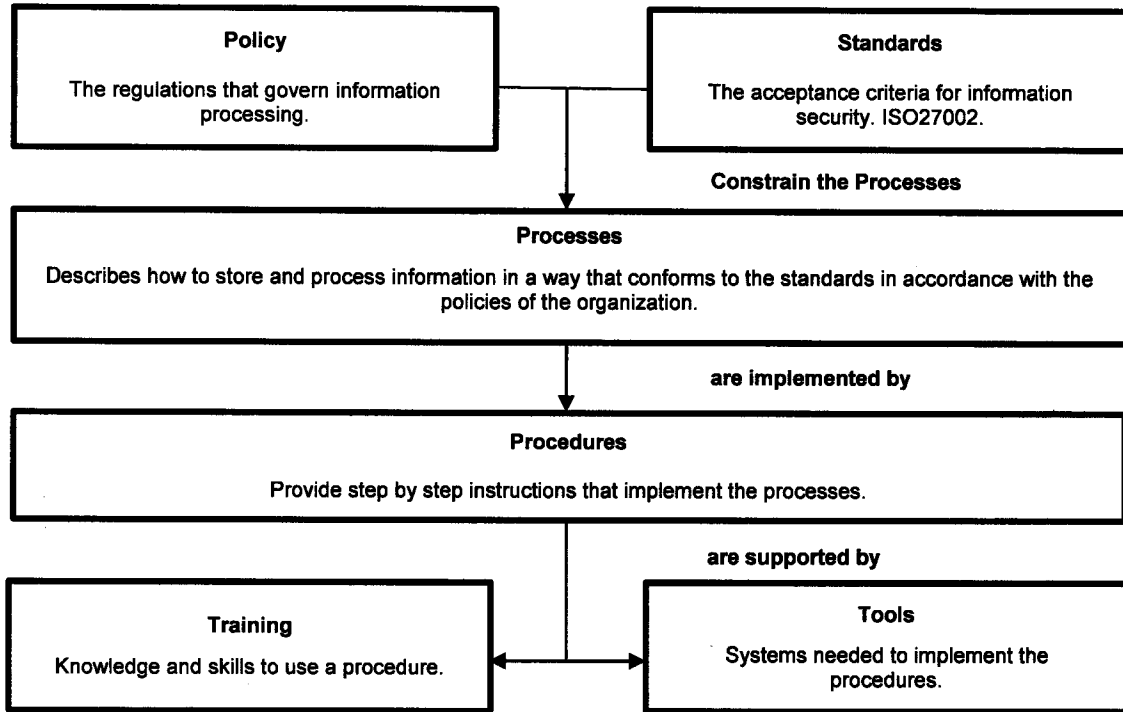


FIGURE ERROR! NO TEXT OF SPECIFIED STYLE IN DOCUMENT.-1: INFORMATION SECURITY POLICY OVERVIEW CHART

5.2 This policy outlines the framework for management of Information Security within the organization.

The Information Security Policy, standards, processes and procedures apply to all staff and employees of the organization, contractual third parties and agents of the organization who have access to the organization's information systems or information.

The Information Security Policy applies to all forms of information including:

- 5.2.1 Hard copy data printed or written on paper
- 5.2.2 Information stored in manual filing systems
- 5.2.3 Communications sent by post / courier, fax, electronic mail
- 5.2.4 Stored and processed via servers, PC's, laptops, mobile devices

5.2.5 Stored on any type of removable media, CD's, DVD's, tape, USB memory sticks and digital cameras.

5.3 Operations Management and Risk

5.3.1 IT Operating Responsibilities and Procedures

IT operating responsibilities and procedures will be documented. Changes to IT facilities and systems will be controlled. Capacity and performance managed, and development, test and operational systems will be segmented, logically or physically to ensure appropriate separation of duties. Separation of duties between Application Development, operational group such as the Help Desk, Network Engineering or Information Delivery Services duties will be clearly defined.

5.3.2 Risk Mitigation

Risk mitigation will be put in place to ensure data and information which is collected, analyzed, stored, communicated and reported upon will not be subject to theft, misuse, loss and corruption.

5.3.3 Logging and Monitoring

Logging and monitoring of system users and administrator/operator activities, exceptions, faults and information security events will be logged and stored allowing future review. System clocks will be synchronized.

5.3.4 Risk Assessment

The organization will undertake risk assessments to identify, quantify, and prioritize risks. Controls will be selected and implemented to mitigate the risks identified.

5.3.5 Vulnerability Management

Vulnerability management will include a patched management program, and there will be rules in place governing software installation by users.

5.4 Security Policy

5.4.1 Information Security Policy Document

The information security policy document sets out the organizations approach to managing information security.

The information security policy is approved by management and is communicated to all staff and employees of the organization, contractual third parties and agents of the organization.

5.4.2 Review

The security requirements for the organization will be reviewed at least annually by the Information Security Officer (ISO). Formal requests for changes will be raised for incorporation into the Information Security Policy, processes, and procedures to be approved by the Chief Information Technology Officer (CITO).

5.5 Organization of Information Security

5.5.1 Statement of Management Intent

- a. It is the policy of the City of Spokane to ensure that Information will be protected from a loss of:
 - i. Confidentiality: so that information is accessible only to authorized individuals.
 - ii. Integrity: safeguarding the accuracy and completeness of information and processing methods.
 - iii. Availability: that authorized users have access to relevant information when required.
- b. The ISO will review and make recommendations on the security policy, policy standards, directives, procedures, Incident management and security awareness education.
- c. Regulatory, legislative and contractual requirements will be incorporated into the Information Security Policy, processes and procedures.
- d. The requirements of the Information Security Policy, processes, and procedures will be incorporated into the organization's operational procedures and contractual arrangements.
- e. Guidance will be provided on what constitutes an Information Security Incident.
- f. All breaches of information security, actual or suspected, must be reported and will be investigated.

- g. Business continuity plans will be produced, maintained and tested.
- h. Information security education and training will be made available to all staff and employees.
- i. Information stored by the organization will be appropriate to the business requirements.
- j. ISMS program review functions done by the CITO and Director of IT and the ISO. An annual review of program objectives requires annual signoff.

5.6 Information Security Coordination

5.6.1 The security of information will be managed within an approved framework through assigning roles and coordinating implementation of this security policy across the organization and in its dealings with third parties.

5.7 Asset Management

5.7.1 The organization's assets will be appropriately protected.

5.7.2 All assets (data, information, software, computer and communications equipment, and service utilities) will be accounted for by the appropriate city department.

5.8 Human Resources Security

5.8.1 The organizations security policies will be communicated to all employees, contractors and third parties to ensure that they understand their responsibilities.

5.8.2 Security responsibilities will be detailed in job descriptions and in terms and conditions of employment.

5.9 Physical and Environmental Security

5.9.1 Critical or sensitive information processing facilities will be housed in secure areas.

5.9.2 The secure areas will be protected by defined security perimeters with appropriate security barriers and entry controls.

5.9.3 Critical and sensitive information will be physically protected from unauthorized access, damage and interference.

5.10 Communications and Operations Management

5.10.1 The organization will operate its information processing facilities securely.

5.10.2 Responsibilities and procedures for the management, operation and ongoing security and availability of all data and information processing facilities will be established.

5.10.3 Appropriate operating procedures will be put in place.

5.10.4 Segregation of duties will be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.

5.11 Access Control

5.11.1 Access to all information will be controlled.

5.11.2 Access to information and information systems will be driven by business requirements. Access will be granted or arrangements made for employees, partners, suppliers according to their role, only to a level that will allow them to carry out their duties.

5.11.3 A formal user registration and de-registration procedure will be implemented for access to all information systems and services.

5.12 Cryptography

5.12.1 Where cryptography requirements exist in order to protect sensitive information for customers, or federal or state requirements require, the organization will use encryption, plus cryptographic authentication and integrity controls such as digital signatures and message authentication codes, and cryptographic key management.

5.13 Information Systems Acquisition, Development and Maintenance

5.13.1 The information security requirements will be defined during the development of business requirements for new information systems or changes to existing information systems.

5.13.2 Controls to mitigate any risks identified will be implemented where appropriate.

5.14 Information Security Incident Management

5.14.1 Information security incidents and vulnerabilities associated with information systems will be communicated in a timely manner.

5.14.2 Formal incident reporting and escalation will be implemented.

5.14.3 All employees, contractors and third party users will be made aware of the procedures for reporting the different types of security incident, or vulnerability that might have an impact on the security of the organization's assets.

5.14.4 Information security incidents and vulnerabilities will be reported as quickly as possible to the ISO and Director of IT.

5.15 Business Continuity Management

5.15.1 The organization will put in place arrangements to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

5.15.2 A business continuity management process will be implemented to minimize the impact on the organization and recover from loss of information assets. Critical business processes will be identified.

5.15.3 Business impact analysis: After action review will be conducted following disasters, security failures, loss of service, and lack of service availability.

5.16 Supplier Relations

5.16.1 The organization will implement policies, procedures, awareness guideline to protect the organization's information that is accessible to IT outsourcers and other external suppliers throughout the supply chain, agreed within the contracts or agreements.

5.16.2 Service delivery by external suppliers should be monitored, and reviewed/audited against the contracts/agreements. Service changes should be controlled.

5.17 Compliance

5.17.1 The organization will abide by any law, statutory, regulatory or contractual obligations affecting its information systems.

5.17.2 The design, operation, use and management of information systems will comply with all statutory, regulatory and contractual security requirements.

6.0 RESPONSIBILITIES

- 6.1 The ISO is responsible for the maintenance and review of the Information Security Policy, processes and procedures.
- 6.2 Heads of Department are responsible for ensuring that all staff and employees, contractual third parties and agents of the organization are made aware of and comply with the Information Security Policy, processes and procedures.
- 6.3 The organization's auditors will review the adequacy of the controls that are implemented to protect the organization's information and recommend improvements where deficiencies are found.
- 6.4 All staff and employees of the organization, contractual third parties and agents of the organization accessing the organization's information are required to adhere to the Information Security Policy, processes and procedures.
- 6.5 Failure to comply with the Information Security Policy, processes and procedures will lead to disciplinary or remedial action, up to and including termination.

7.0 APPENDICES

- 7.1 <https://my.spokanecity.org/opendata/documents/policies/>
- 7.2 <https://my.spokanecity.org/smc/>

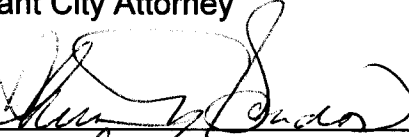
APPROVED BY:



Assistant City Attorney

11/29/17

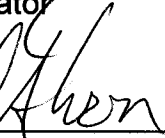
Date



City Administrator

11/30/17

Date



Director - ITSD

11/30/2017

Date