CORPORATE POLICY

Policy Title:	**Information Security Policy**
Policy Category:	**Administration**
Policy No.:	A-010
Department:	**Corporate Services**
Approval Date:	May 9, 2016
Revision Date:	
Author:	SK Ali
Attachments:	None
Related Documents/Legislation:	Security Policy, Records Management Policy, Email Records Management Policy, Confidential Information Policy, Information Security Procedures
Key Word(s):	policy, procedure, security, vulnerability, threat, risk, ISO/IEC 27002

POLICY STATEMENT:

The Corporation of the City of Waterloo is committed to administering and managing an information security policy to protect its information technology assets. This policy outlines necessary security standards, processes and procedures for information and data processing facilities.

PURPOSE:

The purpose of this information security policy is to establish and maintain appropriate security standards, processes and procedures for the protection of City owned information, systems, applications and networks, and to defend against any adverse or unwanted conditions.

Mandatory Policy, *Municipal Act*: No
Policy Administration Team, Review Date: March 9, 2016
Corporate Management Team, Review Date: April 6, 2016

DEFINITIONS:

Availability: Information is available to authorized persons as agreed.

Integrity: Ensuring information has not been altered accidentally or deliberately, and it is accurate and complete.

Information Security: Maintaining confidentiality, integrity and availability of information and data processing facilities.

ISO/IEC 27002 Standards: Defined standards by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC) to manage information security.

Malware: A generic term for a number of different types of malicious code.

Threat: Potential cause of an unwanted incident, which may result in harm to the business.

Vulnerability: The weakness of an asset that can be exploited by one or more threats.

Risk: A combination of the likelihood of an event and its consequence.

Storage media: Devices or other media that store data, application and user information.

SCOPE:

This policy applies to members of the City's organization including members of Council, staff (full-time, part-time and contract), volunteers, Boards, external suppliers, contractors, consultants and anyone else utilizing or accessing the City of Waterloo technology assets.

POLICY COMMUNICATION:

This policy will be made available to staff through the City's website and intranet. It will be communicated to staff via regular updates and through security awareness sessions or posters.

POLICY:

- The confidentiality, integrity and availability of information and data processing facilities must be maintained.

- All users to which this policy applies are responsible for complying with the Information Security Policy and related procedures.

- This security policy shall provide the outline of common security requirements for people and technology that create, maintain, store, access, process or transmit information.

- The Information Security Policy shall be reviewed by the information technology staff once every three years and updated as needed.

- Staff responsible for information technology shall prepare and manage information security procedures based on the ISO/IEC 27002 standards.

- The security procedures will be reviewed annually by the staff responsible for information security, and approved by the director responsible for information technology.

- Exceptions to any security procedure must be documented and approved in writing by the director responsible for information technology.

- Related procedures shall be directly derived from and aligned with the ISO/IEC 27002 standards as listed below.

Information Security Procedures

The information technology staff shall develop security procedures that provide management direction and support essential for the establishment of standards, processes, guidelines and education throughout the corporation. In compliance with ISO/IEC 27002, the City's information security procedures will include, but not be limited to the following security standards and objectives:

IS-1.0 Security Procedures Administration and Organization

This section defines management direction and support based on business requirements and relevant laws and regulations. Essential procedures will define information security roles and responsibilities, and securing use of the City's mobile devices and teleworking.

IS-2.0 Personnel Security

In this section, procedure includes the security awareness, educational program and user responsibilities to comply with the security obligations for information technology assets.

IS-3.0 Asset Management

Asset management objectives are to identify information technology assets, classify information and define user responsibilities to protect assets. Procedures in this section include the asset owner's responsibilities and security requirements to handle storage media.

IS-4.0 Access Control

The procedures in this section define the access management technique based on business requirements, user responsibilities, password rules, segregation of duties and access restrictions to critical systems and applications.

IS-5.0 Cryptography

This procedure outlines the appropriate use of cryptographic algorithms and key management practice to maintain confidentiality, authentication and/or integrity of information.

IS-6.0 Physical and Environmental Security

The procedure in this section covers the physical protection for data center perimeters, access administration and equipment security.

IS-7.0 Operations Security

This section provides essential procedures for operational responsibilities, protection from malware, backup, logging and monitoring, operational software security, technical vulnerability management, and information systems audit events.

IS-8.0 Communications Security

This section describes the information protection rules for communication equipment and data processing facilities. Network security management and information transfer agreement (i.e. non-disclosure) will be included in this security procedure.

IS-9.0 System Acquisition, Development and Maintenance

The procedures in this section outline the security requirements for the procurement of information systems, software development and maintenance, and use of test data.

IS-10.0 Supplier Relationships

This section provides procedures for those instances when the corporation secures the services of suppliers, consultants, contractors and / or outsourcing companies by signing the non-disclosure agreement, access control and change management process.

IS-11.0 Information Security Incident Management

The procedure in this section defines the roles and responsibilities for security respond team and mitigation plan for security incidents.

IS-12.0 Information Security Aspects of Business Continuity Management

This section outlines security requirements for the business continuity program to maintain a secure redundant infrastructure.

IS-13.0 Security Compliance

This section identifies and documents information security obligations including business records, intellectual property, and privacy. This security procedure describes the legal and contractual commitments, security reviews and audits requirements.

COMPLIANCE:

In cases of policy violation, the City may investigate and determine appropriate corrective action.