STRATHCONA COUNTY

Directive

Information Security

References: *Municipal Government Act*, RSA 2000, c M-26
ISO/IEC 27001:2013
Freedom of Information and Protection of Privacy Act, RSA 2000, c F-25

Cross-reference: GOV-003-002D Information Management Directive

Policy Statement

Information is a critical asset of the County. Confidentiality, integrity and availability must be protected in compliance with provincial and federal legal or regulatory requirements.

This Directive shall enable efficient and effective protection of County information assets by implementing an information security management framework: ISO 27001

This will be achieved through a cycle of continuous improvement, and by:

- minimizing information security risk;
- ensuring personnel are trained and knowledgeable;
- applying appropriate security controls; and
- providing protection against business interruptions.

Purpose

The purpose of this Directive is to ensure that appropriate safeguards are in place to protect information and the Information Technology systems, services, end-user equipment and network infrastructure of Strathcona County.

The objectives of Information Security Directive are:

- To secure the County's information assets against theft, fraud, malicious or accidental damage, breach of privacy or confidentiality, financial loss and loss of public trust; and
- To protect the County from damage and liability arising from the use of County computing facilities for any purposes contrary to the County's policies, and provincial and federal legal or regulatory requirements.

Definitions

Information – Data or content recorded or stored in any way, including facts, events, ideas, processes, or concepts, that are specific and organized for a purpose, and to increase understanding within a certain context and timeframe. Includes the summation of all documents, records and data under the control of Strathcona County.

Security – The practice of protecting assets against theft, fraud, malicious, or accidental

damage, breach of privacy or confidentiality, financial loss and loss of public trust.

Facility – Buildings, pieces of equipment, or services that are provided for a particular purpose.

Risk – A probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action.

Security Control – Safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets.

Guidelines

1. Security Awareness Training

Information Technology Services will develop and maintain a security awareness program and ensure that all existing staff and all new staff are made aware of their role in protecting our information and that the awareness program remains current in light of changing technology.

2. Information Security Risk Mitigation

Information Technology Services will develop and maintain an information risk management process that applies an appropriate level of protection based on the sensitivity and value of the information.

3. Security Controls

Information Technology Services will partner with County departments and third party stakeholders to establish and maintain security controls designed to protect the information entrusted to the County by our customers ensuring the integrity, confidentiality and availability of the information.

4. Continuous Improvement

Information Technology Services will be accountable to evolve the County's security program, reporting on Key Performance Indicators (KPIs) that provide feedback on the success of the program.

Policy Record

Date of Approval by Commissioner: Month DD, YYYY

Resolution No: XXX/20XX

Next Review Date: Month DD, YYYY

Policy No: GOV-002-023D

Last Review Date: Month DD, YYYY

Replaces: GOV-002-023 Systems and Data Security

Lead Role: *Chief Commissioner*

Administrative Review: Information Technology Services