Administrative Directive

Cyber Security Administrative Directive

Number: A1473
Department: Financial and Corporate Services

Date of Approval: June 10, 2019
Next Scheduled Review: Date of Approval +3 years

Statement of Directive:
The City expects that all digital assets are kept at an acceptable level of cyber risk, as per the principles set out in this directive. Cyber security risk management aids asset owners with managing cyber risks to digital assets and involves risk identification, risk measurement, mitigation and control, monitoring and reporting.

Definitions:
Unless otherwise specified, words used in this directive and its accompanying procedures have the same meaning as defined in either the City Administration Bylaw, Bylaw 16620 or the COE Cyber Security Glossary.

Purpose:
The purpose of this directive is to proactively manage cyber security risks by establishing principles and accountabilities for digital assets.

Application:
This directive applies to any person who reports to the City Manager or City Auditor and provides services to the City of Edmonton under a contract of employment, contract for the provision of personal services or in the capacity of agent, student, or volunteer.

Accountabilities:
The asset owner is:

- accountable for the digital assets under their custodianship, including the risk exposure;
- accountable for delegating responsibilities for the management of digital assets, including cyber security, under their custodianship;

Asset Owners must comply with all procedures accompanying this directive when making decisions in relation to those digital assets.

By default, the Branch Manager will be designated as the Asset Owner.

The Branch Manager, Open City and Technology is:

- accountable for enforcement of compliance, of known risk, to the Cyber Security Administrative Directive and Administrative Procedure;
- accountable for participating in the risk decisions that impact two or more branches;
- accountable for reporting cyber security risks to the Executive Leadership Team; and
- responsible as a service provider.

The Corporate Information Security Officer, Open City and Technology is:

- accountable for maintaining this directive, as well as supporting administrative procedures, risk reduction strategies, incident response plans and standards;
- accountable for cyber security risk reporting;
- accountable for oversight of all cyber security and cyber security regulations and third party standards;
- accountable for oversight of cyber security incident response; and
- accountable for reporting on the quality control of secure designs for material technology implementations.

Service Providers

- accountable for the secure design and secure operation of the digital asset;
- accountable for cyber security incident response, as per the requirements identified by the Corporate Information Security Officer;
- accountable for providing cyber security metrics and assurances as to the effectiveness of their secure operations;
- accountable for the application of all accepted cyber risk management treatment plans, including ensuring all technology adheres to the cyber security safeguards defined within the City's cyber security standards and supporting work products;
- accountable for providing an annual management attestations demonstrating compliance to the City's cyber security requirements; and
- accountable for obtaining third party attestations, such as SOC1, SOC2, SOC3, from external service providers on an annual basis.

and must comply with all procedures accompanying this directive when making decisions in relation to those digital assets.

Principles:

In carrying out their duties under the procedures accompanying this directive, or when acting in situations not explicitly addressed by an existing procedure, employees will be guided by the following principles:

- Asset owners are accountable for the cyber security of digital assets.
- An asset owner may delegate responsibility but not accountability.
- All roles and responsibilities for cyber security are clearly defined and properly documented.
- The value and sensitivity of digital assets is known, documented and maintained.
- Cyber security legislation and third party standards, such as the Payment Card Industry Data Security Standard, are adhered to.
- Cyber security risks are proactively managed and communicated.