Administrative Policy
Cybersecurity

Program Impacted	Technology and Data *The City of Edmonton's technology and data are leveraged to enable quality decision-making and enhance innovative service delivery*
Number	A1473A
Date of Approval	November 13, 2025
Approval History	June 10, 2019
Next Scheduled Review	November 13, 2029

Policy Statement

The purpose of this policy is to proactively manage cybersecurity risks by establishing principles and accountabilities for digital assets. These principles and accountabilities are the foundations that guide the management of cyber risks

Guiding Principles

Administration will use the following principles when managing cybersecurity risks:

- Asset Owners are accountable for the cybersecurity of digital assets. By default, the Branch Manager will be designated as the Asset Owner.
- Asset Owners must comply with all standards accompanying this policy when making decisions in relation to those digital assets.
- An Asset Owner may delegate responsibility but not accountability.
- All roles and responsibilities for cybersecurity are clearly defined and properly documented.
- The value and sensitivity of digital assets must be defined, documented and maintained.
- Cybersecurity legislation and third party standards are adhered to.
- Cybersecurity risks are proactively managed and communicated.

Accountabilities

- The Asset Owner is:
    - accountable for the digital assets under their custodianship, including the risk exposure; and,
    - accountable for delegating responsibilities for the management of digital assets, including cybersecurity, under their custodianship.

- The Branch Manager, Open City and Technology is:
    - accountable for enforcement of compliance to the Cybersecurity Administrative Policy;
    - accountable for participating in the risk decisions that impact two or more branches;
    - accountable for reporting cybersecurity 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 policy, as well as supporting documentation, risk management strategies, and cybersecurity incident response plan;
    - accountable for cybersecurity risk reporting;
    - accountable for oversight of all cybersecurity, cybersecurity regulations and third party standards;
    - accountable for oversight of cybersecurity incident response; and
    - accountable for reporting on the secure design and implementation of material digital assets.
- Service Providers are:
    - accountable for the secure design and secure operation of their digital assets;
    - accountable for cybersecurity incident response, as per the requirements identified by the Corporate Information Security Officer;
    - accountable for providing cybersecurity 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 cybersecurity safeguards defined within the City's cybersecurity standards and supporting work products;
    - accountable for providing an annual management attestation demonstrating compliance to the City's cybersecurity requirements;
    - accountable for obtaining third party attestations, such as SOC1, SOC2, SOC3, from external service providers on an annual basis; and,
    - accountable for compliance with all standards accompanying this policy when decisions are made in relation to those digital assets.