Proactive Monitoring and Safeguards for Information Systems

The City of Calgary ("The City") protects personal information, data derived from personal information, non-personal data and confidential information ("Information") held across City electronic information systems through a "defense in depth approach": a combination of policies, processes, and safeguards to monitor information systems, identify threats, and prevent unauthorized access. These measures support The City's commitment to protecting privacy while enabling the responsible use of Information to deliver services.

This document describes the alignment of The City's Information protection efforts to the outcomes of the National Institute of Standards and Technology ("NIST") Cyber Security Framework 2.0.

About the NIST Cyber Security Framework 2.0

The NIST framework organizes cyber security activities into six core outcomes. Together, they describe a complete cycle of cyber security risk management.

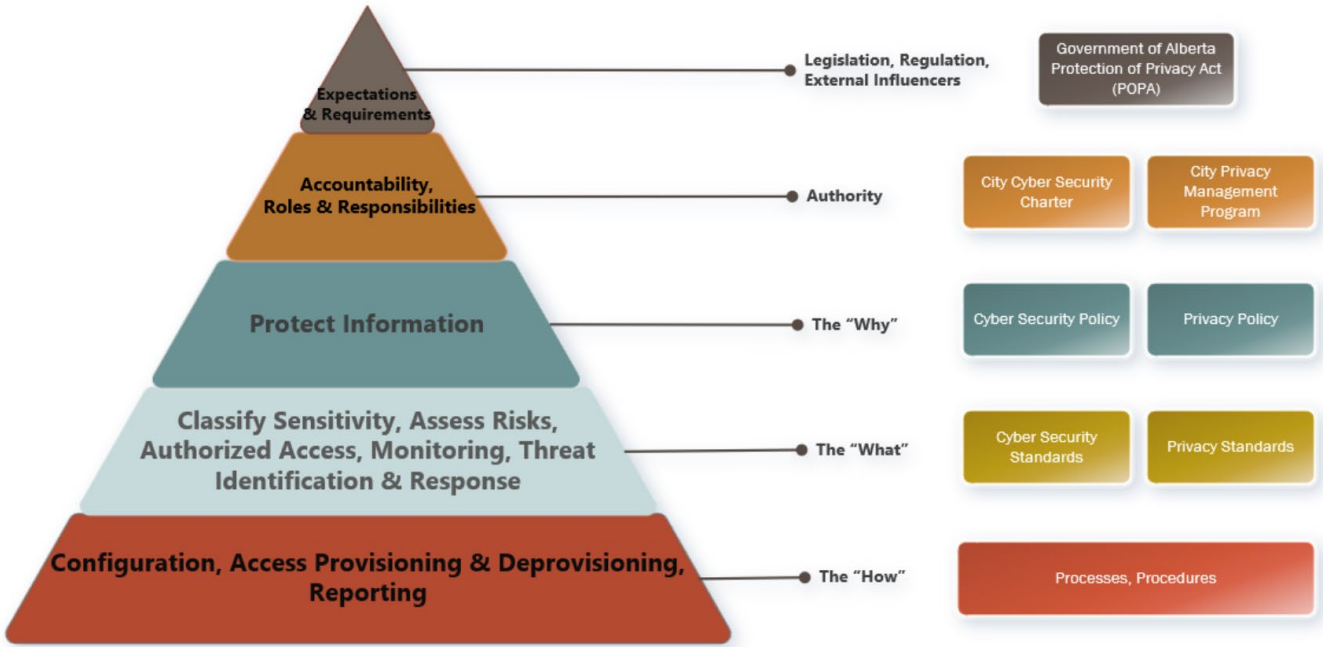
Govern	Identify	Protect	Detect	Respond	Recover
Strategy & Policy	Risk Assessment	Preventive Controls	Monitoring	Incident Response	Restoration

1. Govern – Cyber Security Risk Management Strategy, Policy and Oversight

The Govern outcome establishes and monitors The City's cyber security risk management strategy, expectations, and policies. It provides the organizational context for all cyber security activities.

Policies and Documentation

The City maintains an Administration Policy and Governance Library where cyber security-related policies and standards are published and accessible to employees. A hierarchical structure creates manageable role-based expectations and allows alignment between related functional domains like cyber security and privacy.



Oversight and Accountability

- The City Auditor's Office holds a continuous audit mandate and reviews users' access against authorized users.
- Automated access reviews for cloud environments are monitored through City governance meetings.
- System access requests require documented justification and management approval before access is granted.
- Many business units mandate police background checks as part of their hiring process for City employees who have access to sensitive City systems and information.

2. Identify – Asset Management, Risk Assessment and Supply Chain Risk

The Identify outcome helps The City develop an understanding of its systems, assets, data, and associated cyber security risks, forming the foundation for effective risk management.

Risk Assessments for New or Changed Systems

New technology projects, and any significant changes to existing systems, undergo a cyber security risk assessment before going live. Depending on the system and the Information it holds, this may include one or more of the following:

- Architectural reviews to assess system design and potential risk areas
- Cyber security penetration testing
- Vulnerability assessments
- Web application scanning
- Access control reviews

Systems are also evaluated against The City's Information Security Classification ("ISC") framework to ensure sensitive data, such as personal information and ISC Confidential and Restricted Information, is handled appropriately, and in accordance with its classification.

Vulnerability Management

The City uses automated tools to continuously scan systems to identify known vulnerabilities, allowing us to prioritize patching and updating systems.

Supply Chain Risk Management
When business units procure third-party cloud or software-as-a-service ("SaaS") applications, The City conducts an assessment of the cyber security risks associated with the product, including legal and contract review, before the service is approved for use. Ongoing monitoring responsibilities are defined as part of the procurement process.

Tabletop Exercises
The City conducts regular tabletop exercises to simulate cyber security incidents in a controlled environment. These exercises test The City's response plans, identify gaps in procedures, and build the organizational readiness needed to manage real incidents effectively.

Privacy Compliance and Risk Assessments
A privacy compliance and risk assessment engagement must be completed for any City initiative that involves the collection, use, or disclosure of personal information.

Business Continuity
The City's Business Continuity Planning Policy requires all City business units to maintain up to date business continuity plans, which includes identifying applications used by essential City services and mitigation strategies for various types of disruptions.

Disaster Recovery
The City maintains a Disaster Recovery Plan, focused on recovery of Information assets following a disruptive event.

3. Protect – Safeguards to Prevent or Limit Cyber Security Events

The Protect outcome encompasses the safeguards The City uses to prevent unauthorized access, reduce the attack surface, and maintain accountability for actions taken on City systems.

Administrative Safeguards

- **Automated Access Reviews**
  For most City cloud-based applications, employee access reviews are conducted regularly through automated processes. Supervisors must explicitly confirm whether their direct reports require their current level of access, otherwise access is automatically removed. In some cases, access reviews are performed manually as an ongoing operational maintenance activity by the City division using the service.

- **Cyber Security Awareness Training**
  Employees are required to complete cyber security awareness training on an annual basis. The City also uses simulated phishing attacks to test employees' cyber security awareness.

- **Privacy Awareness Fundamentals Training**
  Employees are required to complete privacy awareness training on an annual basis.

Technical Safeguards

- **User Authentication and Access Controls**
  The City's User Authentication for Enterprise Systems Standard requires defined methods for verifying user identity before access is granted to systems handling personal information, including multi-factor authentication requirements, to reduce the risk of unauthorized access. Multi-factor authentication is also required for remote access to the corporate network. Every user is assigned an individual account, ensuring that actions on City systems can be attributed to a specific person.

- **Change Control**
  Change management processes ensure a standardized approach to maximize efficiency and minimize adverse impacts on IT services and business operations.

- **Firewalls**
  The City uses a layered approach to protect its network and devices, including firewalls to monitor and control traffic.

- **Automated Software Updates**
  Auto-updates are enabled for certain applications across The City's environment, ensuring software remains current and reducing threats.

- **Antivirus Software**
  Corporate antivirus software is deployed across City devices to detect and remove malicious software.

- **Password Controls**
  The City enforces technical controls on passwords across its systems, including requirements for minimum length, complexity, and periodic changes.

- **Encryption**
  Data on portable devices, including phones, tablets, and laptops, is encrypted using full disk encryption or file-based encryption. End user devices, even if not portable, containing sensitive data must use full disk encryption.

- **Email and Web Filtering**
  The City uses email filtering which blocks malicious attachments, suspicious file types and messages based on their content or attributes of the sender. It also uses web-filtering, which stops employees from visiting known malicious or suspicious webpages.

Physical Safeguards

Physical security measures complement The City's digital controls and serve as the foundational layer of protection for Information. Examples include:

- Secured facilities with controlled access to areas where sensitive systems and Information are housed;
- On-site security personnel; and,

- Secure records and Information disposal processes to ensure that physical and digital records containing personal or confidential information are destroyed appropriately.

4. Detect – Timely Discovery of Cyber Security Events

The Detect outcome enables The City to identify cyber security events in a timely manner through continuous monitoring and anomaly detection.

Security Event Monitoring

The City operates a centralized Security Incident and Event Management ("SIEM") system. This platform collects security logs and applies detection rules to identify anomalies or suspicious patterns. Cyber security events are monitored 24/7.

Unstructured Data Monitoring

The City uses dedicated tools to monitor access to files stored on shared network drives. This tooling provides detailed reporting on who is accessing files and when.

Endpoint Threat Detection

The City uses an endpoint threat detection and response tool, which monitors threat indicators, identifies patterns, automatically removes or contains threats, alerts cyber security personnel of incidents, and provides forensic and analysis capabilities. These tools are deployed on workstations, laptops, and servers.

Intrusion Detection Systems

The City employs intrusion detection systems that continuously monitor network traffic for signs of unauthorized access or suspicious activity. These systems generate alerts that are reviewed by cyber security operations staff, enabling timely investigation and response.

Logging and Monitoring User Access

The City requires every user to have their own individual account rather than sharing generic or group accounts. User access to personal information (e.g. viewing, modification, deletion of records) is logged and monitored for various applications in accordance with the Access Control Standard. When possible, The City ensures all locations and systems which contain personal information generate logs which are directed to a security and event monitoring process to identify unauthorized access or suspicious user activity.

5. Respond – Actions Taken in Response to Detected Cyber Security Incidents

The Respond outcome covers The City's ability to take action when a cyber security event is detected — including investigation, communication, and mitigation.

Incident Investigation Capabilities

The City has several capabilities that support effective response when a cyber security incident occurs:

- The centralized SIEM system enables cyber security operations staff to correlate alerts across systems, accelerating investigation and scoping of incidents.
    - Logging across City systems provides activity records to support forensic review when an incident occurs.
    - Individual user account requirements mean that suspicious activity can be attributed to a specific person, reducing investigation time, and improving accountability.

- A structured, approval-based process governs access to sensitive content for the purposes of investigation, with documented rationale and management approval required before access is granted.

Physical Corroboration
Physical security measures have been used to support investigations in situations where digital audit trails were incomplete. This multi-layered approach ensures The City can investigate incidents even when technical records alone are insufficient.

6. Recover – Restoring Capabilities Affected by Cyber Security Incidents

The Recover outcome supports The City's ability to restore normal operations and services following a cyber security incident, and to improve based on lessons learned.

Automated Backups and Data Restoration
The City requires frequent automated backups of City data, with backup frequency and standards defined based on the criticality of the Information. These backups enable The City to restore data to a prior state in the event of accidental deletion or corruption..

Continuous Improvement
The City conducts a post-incident reviews to identify lessons learned and opportunities to strengthen its controls. Findings from these reviews, as well as from tabletop exercises and third-party assessments, are used to update policies, improve technical safeguards, and enhance staff training. This commitment to continuous improvement ensures that The City's cyber security posture evolves alongside the threat landscape.