CITY OF MEDICINE HAT

Policy

Medicine Hat

Title: Cybersecurity			**Number: 0194-2026**
Reference: Administrative Committee July 29, 2026 Corporate Services Committee August 13, 2026	**Adopted by City Council:** September 8, 2026		**Supersedes:** Cybersecurity Policy 0164
	City Clerk	**City Manager**	
Prepared by: Information Technology			

STATEMENT

The City of Medicine Hat is committed to safeguarding its digital assets, protecting sensitive information, and ensuring the confidentiality, integrity, and availability of its systems and data. To achieve this, the City maintains a comprehensive Cybersecurity Framework that establishes robust security measures, promotes user awareness, and fosters a culture of vigilance among employees and interest-holders.

This policy is supported by related governance documents, including the Information Technology Acceptable Use Policy (0195-2026), and by additional standards, procedures, and directives maintained by Information Technology.

PURPOSE

To support consistent oversight, clear accountability, and ensure that cybersecurity risks are identified, assessed, managed, and reported in alignment with the City's strategic objectives, Risk Appetite, and Privacy Management Program.

1. DEFINITIONS

1.1 **Corporate IT** means all City-owned systems, networks, devices, and software, and to any external IT services approved for City use and operated under a contract with the City.

1.2 **Cybersecurity Governance** means the City's practices, structures, and processes for overseeing cybersecurity risk, establishing roles and responsibilities, ensuring policy oversight, and integrating cybersecurity considerations into enterprise decision making.

1.3 **Cybersecurity Governance Group** means the body responsible for overseeing the City's Cybersecurity Governance, ensuring alignment with the Cybersecurity Standards Framework, guiding the Cybersecurity Program,

and providing strategic direction, decision-making support and oversight for cybersecurity risk management.

1.4 **Cybersecurity Incident** means any attempted or actual unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations.

1.5 **Cybersecurity Program** means the Program representing the coordinated approach the City uses to safeguard its information and technology assets by managing risks, implementing security controls, monitoring for threats, and maintaining compliance with relevant laws and standards.

1.6 **Cybersecurity Standards Framework** means the confidential internal reference document that contains detailed cybersecurity standards, directives, and operational procedures that must be followed in order to comply with this policy.

1.7 **Privacy Management Program** means a program maintained by the City as established pursuant to Privacy Management Policy 0193-2026 and applicable privacy legislation.

1.8 **Residual Risk** means the level of cybersecurity risk that remains after security controls have been implemented.

1.9 **Risk Appetite** means the amount and type of cybersecurity risk the City is willing to accept in pursuit of its objectives.

1.10 **Users** means all individuals who are authorized to access and utilize Corporate IT systems. This includes full-time and part-time employees, councillors, Mayor, contractors, consultants, third parties, interns, volunteers, and any other individuals who have been granted access credentials or accounts by the City's IT department.

2. APPLICABILITY

2.1 This policy applies to all Users who access or manage Corporate IT systems or information. This policy does not apply to operational technology (OT) used by the Police, SCADA systems, systems directly supporting SCADA (e.g., Utility Shared Services) or any other systems not under the control of Corporate IT. Systems outside Corporate IT (such as Police or SCADA) remain governed by their own operational policies but must align with Corporate IT cybersecurity requirements when interfacing or exchanging data with Corporate IT systems.

3. AUTHORITY

3.1 Pursuant to Section 201 of the *Municipal Government Act* (Alberta), Council is responsible for developing and evaluating the policies of the City.

3.2 Pursuant to Section 207 of the *Municipal Government Act* (Alberta), the City Manager is responsible for ensuring that the policies of the City are implemented.

3.3 Pursuant to Alberta privacy legislation, the City is responsible for ensuring that information technology systems are secured, protected, and managed in an authorized, appropriate, and compliant manner.

4. PRINCIPLES

4.1 The Chief Information Officer (CIO) is responsible for leading and managing the City's Cybersecurity Program, including identifying and advising on cybersecurity risks and ensuring compliance with applicable legislation.

4.2 The CIO shall be authorized to issue and maintain the Cybersecurity Standards Framework to support the operational implementation of this policy and the City's Cybersecurity Governance practices.

4.3 Cybersecurity risk is an enterprise risk jointly owned by the Executive Leadership Team (ELT) and business area leaders. The CIO coordinates Cybersecurity Governance practices by facilitating risk identification and assessment, documenting risks, and ensuring risks are reported in alignment with the City's Risk Appetite and strategic objectives.

4.4 The CIO is authorized to establish and maintain a Cybersecurity Governance Group to support Cybersecurity Governance practices, including the development of cybersecurity Risk Appetite and ongoing oversight of residual cybersecurity risks.

4.5 The acceptance, transfer, or mitigation of cybersecurity risks is the responsibility of business owners and executive decision-makers, informed by the advice and input of the Cybersecurity Governance Group.

4.6 The Cybersecurity Governance Group functions as an administrative advisory body that supports Cybersecurity Governance practices. It does not replace or duplicate enterprise governance, Council oversight, or the ELT's decision-making authority.

4.7 As the City's Cybersecurity Program matures, its Cybersecurity Governance practices may evolve, and additional governance structures may be established to support effective oversight and enterprise risk management.

4.8 Cybersecurity Governance practices shall be implemented in a manner that supports the City's obligations under applicable privacy legislation and is aligned with the City's Privacy Management Program

5. RESPONSIBILITIES

5.1 Council

(a) Receive, review and adopt this policy and any recommended amendments.

5.2 City Manager

(a) Implement this policy, and ensure the City's Cybersecurity Standards Framework, legal requirements, and compliance obligations are properly established and upheld.

(b) Assign the CIO the responsibility and authority to define, implement, and operate the City's Cybersecurity Program.

5.3 Chief Information Officer (CIO)

(a) Establish and oversee the City's Cybersecurity Program to ensure assets, information, and services are adequately protected.

(b) Ensure the Cybersecurity Program aligns with applicable legislation and the City's Privacy Management Program by implementing proactive security measures, demonstrating due diligence and due care, and meeting mandatory incident reporting requirements.

(c) Ensure the City meets all cybersecurity related obligations under the City's Cybersecurity Program, including but not limited to maintaining required security controls, coordinating incident response activities, ensuring timely reporting, and retaining documentation necessary for compliance processes.

(d) Issue, maintain, and update the Cybersecurity Standards Framework, including directives, operational procedures, and standards essential to implementing this policy.

(e) Support and maintain the City's Cybersecurity Governance practices by coordinating cybersecurity risk management processes, ensuring clarity of roles and responsibilities, and enabling effective oversight through established internal governance structures.

(f) Provide an annual update on key cybersecurity risks, compliance status, significant cybersecurity activities, and any accepted Residual Risks to the designated internal committees during a closed session, in accordance with established committee processes.

(g) Socialize annually to the Executive Leadership Team (ELT) any changes or additions to the Cybersecurity Standards Framework.

6. NON-COMPLIANCE

6.1 Non-compliance with this policy or the standards and directives within the Cybersecurity Standards Framework may result in disciplinary actions, up to and including termination of employment or contracts.

Related Documents

The documents below are listed for convenience and cross-reference purposes only. This non-exhaustive list does not form part of the policy and may be updated administratively from time to time.

- Records Management Policy 0156
- Privacy Management Policy 0193-2026
- Information Technology Acceptable Use Policy 0195-2026
- Cybersecurity Standards Framework (internal use only)