CITY OF MEDICINE HAT

Policy

Medicine Hat

Title: Information Technology Acceptable Use			Number: 0195-2026
Reference: Administrative Committee July 29, 2026 Corporate Services Committee August 13, 2026	**Adopted by City Council:** September 8, 2026		**Supersedes:** Information Technology and Acceptable Use Policy 0163
	City Clerk	**City Manager**	
Prepared by: Information Technology			

STATEMENT

The City of Medicine Hat recognizes the importance of using Information Technology (IT) systems to conduct City business in a manner that protects the interests of the City and its interest-holders. City of Medicine Hat IT systems must be used in a manner that protects City information, IT assets, user privacy, and the City's reputation. Corporate IT systems shall be used exclusively for approved City business purposes, except where limited personal use is specifically permitted under this policy.

PURPOSE

To establish expectations for acceptable use of Corporate IT in order to protect security, privacy, operational integrity, and the City's reputation.

1. DEFINITIONS

1.1 **AI Services** means any software, application, platform, tool, or Cloud Based Service that uses artificial intelligence, machine learning, generative AI, automated decision-making, or similar technologies to create, process, analyze, summarize, classify, predict, recommend, or otherwise manipulate information, whether free or paid and whether accessed through Corporate IT or personal devices.

1.2 **Cloud Based Services** means services offered by third-party vendors that are hosted, managed, and operated on infrastructure not controlled by the organization and accessed over the internet, whether free or paid, regardless of whether the data is stored inside or outside of Canada.

1.3 **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. For the purposes of this policy, it does not

include city-provided, publicly accessible IT services such as free Wi-Fi networking in City premises.

1.4 **Shadow IT** means the acquisition, deployment, or use of IT systems, software, services, or Cloud Based Services for City business without approval from the IT Department.

1.5 **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, 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 and third parties 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 the use of information technology systems is authorized, appropriate, and compliant.

4. PRINCIPLES

4.1 Corporate IT systems, devices, and software are acquired and operated to support City business. Only approved devices and software may be connected to the City internal networks, used to store or process City information, or conduct City business.

4.2 Only software applications approved by the Information Technology department may be used to store and process City information or conduct City business.

4.3 City information, including information about City residents, must not be stored in, transmitted to, or processed by unapproved Cloud-Based Services or AI Services.

4.4 Users must not deploy or use unapproved software, browser extensions, AI Services, Cloud Based Services, Shadow IT, or online services for City business unless approved in accordance with the City's Cybersecurity Policy and related framework, administrative standards, directives, or guidelines.

4.5 Users may make reasonable, limited personal use of Corporate IT services, provided such use is minimal, compliant with laws and policies, non-intrusive, and does not involve the storage of sensitive City information. The City does not back up, protect, or assume responsibility for any User-owned personal information, applications, or accounts installed or accessed by Users on City-owned devices, regardless of whether such devices are used for limited personal purposes.

4.6 Personal devices may access City public Wi-Fi networks for personal use and may access City-approved Cloud-Based Services for convenience, provided that no sensitive City information is stored on the personal device. Personal devices are not intended to serve as a primary means of conducting City business unless explicitly approved. Users must comply with this policy when using personal devices on City public networks or with City data.

4.7 The City may implement technical controls such as a web site, web content, or protocol filters to prevent the use of IT systems that are unacceptable or dangerous. However:

(a) filtering systems are implemented for security and operational purposes; however, Users must not assume that an unblocked website or service is acceptable for City use. Users are responsible for ensuring their actions comply with this policy, regardless of whether technical controls prevent access;

(b) Users must use judgment in deciding what uses of City resources are acceptable and will be held accountable for their decisions; and

(c) any attempt to bypass these controls is strictly prohibited.

4.8 City systems are monitored for operational and security purposes, and all communications, information, and activities may be observed and recorded as necessary for authorized operational, security, compliance, or investigative purposes.

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.

5.3 Chief Information Officer (CIO)

(a) Establish governing standards and directives within the City Cybersecurity Standards Framework to clarify and enforce this policy.

(b) Approve, and regularly review, any justified requests for exceptions to the Cybersecurity Standards Framework.

5.4 Department Directors

(a) Ensure that staff within their departments understand and comply with this policy and related cybersecurity standards and directives within the Cybersecurity Standards Framework.

(b) Support the implementation of IT controls and enforce corrective action where violations occur.

(c) Ensure that access to Corporate IT resources for new hires, contractors, or departing staff is requested, modified, and revoked in a timely manner.

(d) Report suspected misuse or security incidents to Corporate IT department immediately.

5.5 Information Technology Managers

(a) Ensure that Third-Party Service Providers accessing Corporate IT Systems or City information are approved through established City processes.

(b) Ensure that Third-Party access is appropriate, limited, and removed when services are no longer required.

(c) Report suspected misuse or security incidents involving Third-Party Service Providers to Corporate IT immediately.

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
- Cybersecurity Policy 0194-2026
- Cybersecurity Standards Framework (internal use only)