MEDICINE HAT COLLEGE

PROCEDURE

Procedure Name	**SECURITIES AND PROTECTION** *Revised*		
Procedure Number	**IT 2.3**	Approval Date	May 13, 2026
Parent Policy	IT 2.0 Digital Security and Technology Management		
Procedure Authority	Director, Information Technology		
Executive Sponsor	Vice-President, Administration and Finance		
Approved By	Vice-President, Administration and Finance		

1. PURPOSE

Medicine Hat College (MHC) protects its digital infrastructure to ensure the security, integrity, and availability of systems, data, and services. Established and consistent administrative and technical safeguards protect digital systems and information from unauthorized access, misuse, loss, or disruption. These measures foster a resilient digital environment that enables teaching, learning, research, and administration while supporting the college's operational responsibilities and risk management obligations.

2. SCOPE

This procedure applies to all MHC systems, networks, devices, and services that store, process, or transmit institutional data and to all employees, contractors, and other individuals who use those systems.

3. DEFINITIONS

- **Administrative Controls:** policies, procedures, and standards that guide organizational behaviour and practices, and set requirements.
- **Automated Controls:** system or software-based measures that ensure continuous enforcement and rapid response such as access restrictions, intrusion detection, or automated backups.
- **College Corporate Network:** the college's centrally managed, on-premises network environment used to access internal systems, services, and data intended for official college business. Access to this network is restricted to college owned and IT managed devices that meet the college's security and compliance standards.
- **Engineered Controls:** physical or technical measures designed to prevent or reduce risk through system design, such as multi-factor authentication or authentication accounts.
- **Information Technology Resource (IT Resource):** any hardware, software, digital service, account, or computing system owned or managed by the college that creates, stores, processes, transmits institutional data, or connects to a college network. If you are unsure if something is an IT resource, contact ITS.

4. ADMINISTRATIVE SECURITY CONTROLS

Administrative security controls are policies, procedures, standards, and practices that manage human behavior and organizational processes to protect the college's digital systems and

information. These controls support accountability, risk reduction, and compliance, and direct employees, contractors, and other authorized users to act in a secure and responsible manner.

4.1. **Training and Safe Use**

4.1.1 Cybersecurity training is available for all employees and authorized users of college digital systems.

4.1.2 This training provides guidance on safe handling of credentials, proper use of college systems, and recognition of security threats such as phishing and social engineering. Users are instructed on how to protect institutional information, handle suspected security incidents, and follow acceptable use practices. Training is documented, tracked, and refreshed at regular intervals to ensure ongoing awareness and compliance with procedural requirements.

4.1.3 By fostering a culture of safe use, the college reduces the likelihood of human error compromising digital security.

4.2. **Auditing**

4.2.1 Audits are structured assessments that determine whether MHC policy, procedures, standards, and processes are being followed as intended and are achieving their objectives. They may include internal and external evaluations.

4.2.2 Information Technology Services (ITS) utilizes audit results to support continuous improvement by:

- verifying administrative controls remain effective over time,
- identifying needed adjustments in response to changing technology, legislation, organizational structure, or risk environment, and
- informing updates to policy, procedures, standards, and processes to maintain compliance and operational resilience.

4.3. **Incident Response**

4.3.1 The IT Security Team is responsible for coordinating the investigation and management of incidents in accordance with the Incident Response Plan (IRP). Incident response activities include initial response, communication protocols, containment and eradication, evidence collection, recovery, restoration, and prevention or recurrence.

4.3.2 Post-incident reviews are conducted to capture lessons learned and improve administrative and engineered controls, ensuring continuous improvement in the college's security posture.

5. ENGINEERED SECURITY CONTROLS

Engineered security controls are system or software-based controls implemented to prevent, detect, or mitigate security threats. These controls complement administrative measures by providing automated protections, monitoring capabilities, and enforcement mechanisms that safeguard the integrity and availability of institutional systems, resources, and data.

5.1. **Connections and Remote access**

5.1.1 Internet facing systems and applications are protected utilizing a layered approach to security controls.

5.1.2 Certain services are only accessible through the College Corporate Network or secure gateways to reduce exposure, enforce stronger authentication, and protect sensitive data.

5.1.3 Remote access to on-campus IT resources is only permitted through ITS approved access methods.

5.1.4 Geo-blocking may be applied to restrict access, helping prevent unauthorized activity and automated attacks. Users traveling to blocked regions must contact ITS for access.

5.1.5 In order to reduce risk, certain activity may be prohibited on the college's internal operational and business systems. To support other use cases, such as sensitive research requirements, which might be otherwise restricted, ITS will work to find suitable solutions where applicable.

5.2. **Content Filtering**

5.2.1 Content filtering may be employed to maintain the security, integrity, and safe use of IT resources. Filters may limit search results or restrict access to internet sites identified as high security risks. Personal devices connected to college networks are subject to the same filtering rules.

5.2.2 ITS will not engage in URL filtering or content blocking solely for the purpose of censorship.

5.2.3 Requests for access to filtered internet content may be submitted to the IT Support Centre for vetting and approval from the Director, IT.

5.3. **Antivirus Controls**

5.3.1 All college-managed systems and devices are protected by malware detection and prevention tools that provide real-time scanning and regular updates to defend against emerging threats. Updates to these tools are performed regularly to ensure timely protection.

5.3.2 Malware protection complements user awareness training by mitigating the risk posed by inadvertent exposure to malicious content.

5.3.3 While malware protection may occasionally impact performance, these measures are essential to maintain security and operational integrity.

5.4. **Bandwidth Management**

5.4.1 The college may implement measures to manage bandwidth usage across its internal network and external connections. These controls help maintain network stability, support instructional and business continuity, and reduce the impact of congestion or misuse on overall network performance.

6. PASSWORD CONTROLS

6.1. Password security relies on a combination of engineered and administrative controls. Engineered controls enforce secure authentication across college systems, while administrative controls outline password requirements. The System Account Password Standard defines the required characteristics for password strength, protection, and update schedule. Engineered controls apply these requirements consistently wherever college credentials are used.

6.2. Multi-factor authentication (MFA) is implemented to further strengthen identity verification and reduce the risk of unauthorized access.

6.3. Passwords are confidential and must not be shared, disclosed, or hinted to anyone, including ITS employees or supervisors. They must not be stored or transmitted insecurely. When storage is unavoidable, ITS approved secure methods must be used.

6.4. These measures protect the confidentiality and integrity of authentication processes by preventing weak or compromised passwords and ensuring credentials are handled securely.

7. BACKUP AND CONTINUITY

7.1. ITS maintains backup and continuity measures to ensure the availability, recoverability, and resilience of digital systems, data, and services. These measures protect against data loss, system failures, and disruptions caused by security incidents or other operational events.

7.2. Backups are performed regularly by ITS according to defined schedules and will adhere to college retention and disposition requirements. They include critical system configurations, databases, applications, and institutional information. Backup integrity is verified periodically to ensure that data can be reliably restored when needed.

7.3. Continuity planning ensures that essential digital services remain available or can be quickly restored following disruptions. By maintaining robust backup and continuity practices, the college minimizes the impact of security incidents, supports operational resilience, and ensures that teaching, learning, research, and administrative activities can continue without unnecessary interruption.

7.4. ITS will maintain and may regularly test recovery plans for power outages, cyberattacks, and other distributions to ensure critical services can be restored quickly.

7.5. For cloud-based systems, data backup and disaster recovery services, including testing are managed by contracted vendors. The college is accountable for conducting risk-based reviews of vendor backup and disaster recovery controls through the Outsourced Risk Assessment (ORA) process to ensure they meet MHC risk, continuity, and assurance requirements.

ORIGINAL COPY SIGNED

_____

Wayne Resch
Vice-President, Administration and Finance
Date: May 13, 2026

Additional Information	Location
System Account Password Standard	MHC Website (internal only)/Policy & Procedure SharePoint

MHC ERM

RISK ID: 4.2 Availability and Continuity; 4.3 Integrity; 4.6 Adequacy of IT Infrastructure; 4.8 Data, Privacy and Security