MEDICINE HAT COLLEGE

POLICY

Policy Name	**DIGITAL SECURITY AND TECHNOLOGY MANAGEMENT** *Revised*				
Policy Number	IT 2.0	Category	Information Technology		
Policy Authority	Director, Information Technology		Approval Date	May 13, 2026	
Executive Sponsor	Vice-President, Administration and Finance		Next Review Date	May 13, 2031	
Approved By	President and CEO		Frequency of Review	Every 5 Years	

1. POLICY STATEMENT

Strong digital security and management of Medicine Hat College (MHC) Information Technology (IT) systems, resources, and data minimizes institutional risk, upholds confidentiality, and enables secure and efficient operations while safeguarding critical assets. This resilient infrastructure fosters trust, supports regulatory compliance, and empowers the organization to thrive in a secure digital environment.

2. SCOPE

This policy applies to all institutional digital systems, services, and hardware and those who access or manage these resources.

3. DEFINITIONS

- **Administrative Controls:** policies, procedures, and standards that guide organizational behavior 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.
- **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. PRINCIPLES

4.1 MHC's digital security and technology management approach is an integration of engineered, administrative, and automated controls that together reduce risk, support compliance, and enhance operational resilience.

4.2 The college is committed to protecting the confidentiality, integrity, and availability of its information systems and digital assets. These core principles guide all digital security efforts to ensure that information and the systems and services that use it, are up to date, are accurate, accessible to authorized users, and protected from unauthorized access or loss.

4.3 The college prioritizes security and prevention of obsolescence as institutional values that are essential to responsible technology stewardship, ensuring inclusion across all stages of the technology lifecycle. Protective technologies, evergreening, and established controls are

applied to ensure systems remain efficient and secure across their full lifecycle, from planning and procurement through to decommission.

4.4 Digital security is a shared responsibility that depends on the active participation of all members of the college community. Individuals are accountable for understanding and upholding their responsibilities regarding the protection of systems and data. The college provides resources and training, but it is the responsibility of each user to act ethically, follow security requirements, and contribute to a secure digital environment.

4.5 The college monitors and manages IT resources to maintain optimal performance, security, and reliability. Through regular updates, patching, and technology evergreening, the college mitigates vulnerabilities and extends the useful life of digital assets in alignment with operational and security requirements.

4.6 The college values privacy, transparency, and trust in all technology practices. Employee account monitoring is undertaken only when necessary for investigations or security incidents and follows a formal process, including documented authorization and executive approval.

4.7 Information and Technology Services is responsible for implementing and enforcing digital security rules through an approved set of standards. These standards are established under the authority of this policy and related procedures, ensuring a consistent, accountable, and policy-aligned application of security controls across all systems and users.

ORIGINAL COPY SIGNED

Kevin Shufflebotham
President and CEO
Date: May 13, 2026

ORIGINAL COPY SIGNED

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

Additional Information	Location
IT 2.1 Resource Allocation & Lifecycle Management Procedure	MHC website/Policy & procedure SharePoint
IT 2.2 Systems and Resource Monitoring Procedure	MHC website/Policy & procedure SharePoint
IT 2.3 Securities and Protection Procedure	MHC website/Policy & procedure SharePoint