MEDICINE HAT COLLEGE

POLICY

Policy Name	**GOVERNANCE AND ACCESS MANAGEMENT** *Revised*			
Policy Number	IT 1.0	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

Effective governance of technology is vital to ensuring that Information Technology (IT) systems and services operate reliably and align with Medicine Hat College's (MHC) strategic objectives. The principles of transparency, accountability, and proactive management guide the deployment, maintenance, and oversight of technology resources, mitigating risks, and creating value across all departments. Structured processes for change, risk management, and incident recovery, safeguard continuity and minimize disruptions, ensuring college systems remain secure, responsive, and supportive.

2. SCOPE

This policy governs the management of institutional IT systems and data, setting rules for access, roles, and decision-making authority, and applies to all users and resources.

3. DEFINITIONS

- **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 Information Technology Service.
- **Users:** any individual that accesses or uses IT resources. This may include, but is not limited to, employees, students, contractors, vendors, volunteers, third-party service providers, and guests who are granted temporary access for events, conferences, or campus visits.

4. PRINCIPLES

4.1 Governance of digital technology is recognized as a strategic function within the college. The Director, Information Technology Service (ITS), Executive Committee, and the Senior Leadership Team are accountable for aligning technology initiatives with the college's mandate and goals, managing associated risks, and ensuring responsible stewardship of IT resources and investments.

4.2 The IT Control Framework governs all ITS operations in alignment with the MHC Enterprise Risk Management Framework, ensuring risks are identified, mitigated, and managed in a manner consistent with institutional priorities.

4.3 The college is committed to meeting all legal, regulatory, and contractual obligations related to information security and data protection. Digital security practices will adhere to applicable legislation, industry standards, and best practices to ensure compliance and accountability.

4.4 MHC values transparency and cross-functional collaboration where possible. Strategic technology decisions are informed by meaningful input from users, fostering shared understanding and promoting compliance with legislation, standards, and best practices.

4.5 Clear standards and procedures manage risk, security, compatibility, and operational efficiency within MHC digital environments. They are supported by this policy and are regularly reviewed and updated to reflect technological advancements and emerging security threats, ensuring a secure and consistent user experience.

4.6 Regular reviews, assessments, and benchmarking of systems, hardware, access and governance documents allow MHC to remain current, effective, and resilient in a rapidly evolving digital environment. This ongoing commitment enables the college to proactively adapt to new challenges and opportunities, fostering sustainable excellence over time.

4.7 The college is committed to a structured change management process for all critical IT services and assets. Changes will be planned, communicated as necessary, scheduled, and approved by designated authorities to minimize disruption and maintain service integrity. Documentation will be maintained to enable accountability, auditability, facilitate review, and support the ability to revert changes if necessary.

4.8 A risk-based approach underpins the college's digital security strategy. Controls and assessments are used to identify, evaluate, and mitigate risks to existing and potential systems, services, data, and users in a manner that is proportional, effective, and aligned with institutional priorities.

4.9 MHC's structured incident response plan, supported by an Incident Response Committee, ensures rapid detection, containment, investigation, recovery, and post-incident learning to reduce the impact of security events and prevent recurrence.

4.10 Access to information is provided only to those who need it and will be revoked when it is no longer required, ensuring only authorized people can access the required information at the appropriate time.

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 1.1 Acceptable Use Procedure	MHC Website/Policy & Compliance SharePoint
IT 1.2 Data Storage and Use Procedure	MHC Website/Policy & Compliance SharePoint
IT 1.3 Risk Assessments for Outsourced Services Procedure	MHC Website/Policy & Compliance SharePoint
IT 1.4 Responsible Use of AI Procedure	MHC Website/Policy & Compliance SharePoint