MEDICINE HAT COLLEGE

PROCEDURE

Procedure Name	**SYSTEMS AND RESOURCE MONITORING** *Revised*		
Procedure Number	**IT 2.2**	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) is committed to ensuring the performance and proper use of its technology systems and services. Monitoring of information technology (IT) resources is undertaken to support safe, effective, and efficient operations, maintain system and services security and reliability, and uphold institutional compliance.

2. SCOPE

This procedure applies to all IT resources and all individuals who use or manage those resources.

3. DEFINITIONS

- **Content Filtering:** the use of technical controls to restrict or limit access to certain internet sites or categories of content based on security risk, legal requirements, or operational needs.
- **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.
- **Operational Monitoring:** focuses on the performance, availability, reliability, and backup of institutional data to ensure IT resources function as intended.
- **Security Monitoring:** detects, investigates, and responds to potential threats, unauthorized access, or vulnerabilities that could compromise systems or data. It is conducted in a secure and accountable manner. Monitoring will be proportionate to the risk or threat.
- **Targeted Monitoring:** monitoring of IT resources and employee accounts in response to suspicious user activity, security events, or other authorized investigations, and is limited to systems, accounts, or data relevant to the investigation.

4. GENERAL

4.1 Monitoring is conducted for defined operational, security, compliance, or investigative purposes and is not used for continuous or routine surveillance of users.

4.2 Any monitoring undertaken by Information Technology Services (ITS) balances institutional security with respect for individual privacy. Monitoring activities are governed through college polices, procedures, standards, and legislation to ensure accountability, consistency, and alignment with legal and ethical obligations.

4.3 Information obtained through monitoring is managed as a confidential institutional record and protected against unauthorized access or secondary use.

4.4 ITS is obligated to notify proper authorities including law enforcement agencies of any use of the system suspected of being illegal. This requirement to report is mandatory.

5. OPERATIONAL MONITORING

5.1 Operational monitoring is conducted by authorized ITS employees using system logs, dashboards, alerts, auditing, and automated reporting tools.

5.2 Monitoring is limited to what is necessary to maintain system operations.

5.3 User activity is reviewed only as required to support resource performance.

5.4 Information content stored and transmitted in college systems will not be accessed without necessity, due process, and notification for the purposes of operational monitoring.

6. SECURITY MONITORING

6.1 Security monitoring is conducted by authorized IT employees and is prompted by automated alerts generated from security event logs, intrusion detection tools, network monitoring, and vulnerability scanning.

6.2 Monitoring is limited to institutional IT resources and is proportionate to the threat or risk level.

6.3 In the event of security related incidents, ITS may need to review information stored or transmitted in systems including file systems, cloud services, email, or other resources. This access will be carried out by authorized employees, follow ITS incident response process, and will be documented.

6.4 If monitored user accounts are involved in or locked as a result of a security incident, ITS will contact users in a timely manner to notify them and provide guidance on how to restore access.

7. TARGETED MONITORING

7.1 Targeted monitoring itself is not disciplinary, any use must be carried out as part of an investigation under an applicable human resources, student conduct, academic integrity, or other college policy. It requires reasonable grounds and is only used for approved observation.

7.2 Targeted monitoring is conducted with proper authorization, adheres to the intended purpose, and is transparent wherever appropriate.

7.3 Direction for targeted monitoring comes from the department carrying out the investigation and requires documented approval from the applicable department head or executive as well as ITS assessment, and Human Resources consultation when applicable, before execution.

7.4 Monitoring is limited to the approved investigative scope; any unrelated data or resources are excluded. All monitoring activities are documented, stored securely, and access controlled.

8. EMERGENCY MONITORING

8.1 In circumstances where there is an immediate and significant risk to institutional systems, individuals, or operations, ITS may initiate limited monitoring without prior authorization.

8.2 Emergency monitoring actions must be:

(a) time-limited and narrowly scoped,

(b) documented as soon as practical, and
(c) subject to retrospective review.

ORIGINAL COPY SIGNED

_____

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

MHC ERM

RISK ID: 4.2 Availability and Continuity; 4.3 Integrity; 4.8 Data, Privacy and Security