MEDICINE HAT COLLEGE

PROCEDURE

Procedure Name	**RISK ASSESSMENT FOR OUTSOURCED SERVICES** *Revised*		
Procedure Number	**IT 1.3**	Approval Date	May 13, 2026
Parent Policy	IT 1.0 Governance and Access 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 protecting the confidentiality, integrity, and accessibility of institutional data by identifying and assessing any risks associated with outsourced services. Responsible stewardship of information protects students, employees, and MHC's reputation while enabling accountable use of third-party systems and services.

2. SCOPE

This procedure applies to all outsourced systems that house MHC institutional data.

3. DEFINITIONS

- **Institutional Data**: data owned by the college or for which the college is responsible. This includes but is not limited to internal, confidential, restricted, personal, and high-sensitivity data as defined in the Data Classification Standard.
- **Outsourced Service Provider:** for the purposes of this procedure, an outsourced service provider is any external organization or vendor that stores, processes, or otherwise houses MHC owned or stewarded data on its information systems.

4. PRINCIPLES

The following principles reflect the college's commitment to responsible stewardship, risk awareness, and the protection of institutional data when using outsourced services.

(a) Data Stewardship: the college treats all institutional data as a valuable asset and ensures it is stored and processed responsibly.

(b) Risk Awareness: decisions to use outsourced services are guided by a clear understanding of potential risks and their impact on the institution.

(c) Security by Design: risk assessments are performed before any data is shared, embedding security and privacy considerations into every stage of service adoption.

(d) Continuous Assurance: risk reviews are conducted regularly to ensure ongoing protection and compliance as services evolve.

(e) Regulatory Compliance: assessments of outsourced services incorporate information and privacy legislation requirements including Government of Alberta audit and compliance requirements, as well as Privacy Impact Assessments (PIAs) as necessary.

5. PROCESS

5.1. The Director, Information Technology (IT), or designate, will initiate this process for any new or existing outsourced service requiring review.

5.2. The Director IT or designate, will work with relevant Information Technology Services (ITS) and operational area employees to assess the risks of an outsourced provider from a security and privacy perspective, and consider ways to mitigate risks if needed.

5.3. The Outsourced Risk Assessment (ORA) form, based on the college's Enterprise Risk Management process, will be completed to evaluate the service.

5.3.1 Risk severity is calculated from likelihood (probability of a risk event) and impact (consequence if the risk occurs).

5.3.2 When provider controls are unknown, likelihood is assessed using a worst-case assumption and adjusted based on available evidence.

5.3.3 All ratings and reasoning must be documented to support future reviews.

5.4. In cases with a residual risk level within the risk tolerance, the completed ORA is sufficient to indicate authorization for the use of the outsourced service.

5.5. If residual risk exceeds tolerance after mitigation considerations, the recommendation would be that the service is not used. The Director IT will provide that official recommendation to the data owner and the Executive Committee (EC) member responsible for ITS, including any already considered or recommended mitigation measures. EC has the authority to accept the risk, regardless of the recommendation, but it must be documented in writing and be retained with the ORA.

5.6. If an outsourced provider is approved through this process, a PIA may also be required before a provider can be authorized in totality.

5.7. ORAs, recommendations from the Director IT, and EC approvals will be stored in a centralized ITS location for as long as required.

ORIGINAL COPY SIGNED

_____

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

Additional Information	Location
Outsourced Risk Assessment Form	Internal ITS Document, available upon request

MHC ERM
RISK ID: 4.1 Security and Access; 4.8 Data, Privacy, and Security