

1.0 POLICY STATEMENT

- 1.1 MacEwan University (“University”) is committed to protecting the confidentiality, integrity and availability of the data, information systems and networks in its custody or under its control through the creation, implementation and enforcement of information security standards and procedures.

2.0 PURPOSE

- 2.1 This policy provides a structured framework for safeguarding the University’s information technology assets and sensitive data from cyber threats. It sets standards, roles, and response protocols to protect the confidentiality, integrity, and availability of sensitive information and systems. The policy supports academic and operational continuity, promotes responsible use of technology, ensures compliance with regulatory requirements, and nurtures a culture of awareness and accountability across the University.

3.0 APPLICABILITY

- 3.1 This policy applies to all Members of the MacEwan Community.

4.0 DEFINITIONS

Baseline

A specific standard, explicit to a technology, usually a software or hardware build or deployment that includes the steps required to secure the technology.

Members of the MacEwan Community

Those persons involved in conducting University-related activities or using University property (eg. students, Faculty, staff, contractors, and all visitors while they are on University property or are using its facilities).

5.0 POLICY ELEMENTS

5.1 Guiding Principles

- 5.1.1 The University reserves the right to manage access to, and use of, all information owned, created or controlled by the University, all information technology assets owned, leased, managed or subscribed to by the University, and all services provided by the University, both internal and to external entities.
- 5.1.2 The Information and Technology Services (ITS) department shall ensure that all information security Baselines, standards, operating procedures and other relevant security controls are developed, enforced, regularly maintained and monitored for compliance and efficacy.
- 5.1.3 All information, such as contact lists, files, folders, email attachments and emails, sent or received on University email systems is proprietary to the University and therefore considered to be University property for records retention, legal and data security purposes.
- 5.1.4 All devices that connect to the University network are subject to monitoring and/or auditing.
- 5.1.5 A regular mandatory Cyber Security and Privacy training program will be administered, repeated annually, and tracked for all Members of the MacEwan Community.

- 5.1.6 Regular information security testing and risk assessments will be performed and tracked to ensure compliance with established Baselines and to help minimize exposure to security risk due to changes within the environment, advancements in detection capabilities or newly identified threats to the organization.
- 5.1.7 Metrics suitable to demonstrate the efficacy of the overall information security program will be developed, maintained, and reported to the Board of Governors.
- 5.2 To ensure the protection and security of our computing environment, ITS has implemented an Information Security program comprising of the following key elements:
 - 5.2.1 All information under the custodianship of the University must be classified and handled in accordance with the *Data Classification Standard* to ensure the consistent application of appropriate security controls.
 - 5.2.1.1 Classified information must not be disclosed to unauthorized third parties, must be processed and transmitted within secure environments appropriate to its sensitivity, and must be safeguarded to ensure that access is restricted to authorized recipients only.
 - 5.2.2 Cryptographic technologies utilized by the University are in accordance with established best practices to ensure effective key management. These technologies facilitate the secure key lifecycle management, including generation, distribution, usage, storage, and destruction.
 - 5.2.2.1 User accounts and IDs that are granted access to resources on the University network must be unique, authorized, authenticated, and managed through the creation of standards and procedures governing the authorization, creation, amending, suspending, removal, and review of account and access privileges.
 - 5.2.2.2 File shares and folder access shall be carefully controlled and monitored ensuring that only authorized personnel may have access to stored information.
 - 5.2.2.3 When the sensitivity of the data or the mobility of the device requires additional protection, a centrally managed cryptographic mechanism must be implemented to encrypt all data stored on the device.
 - 5.2.3 Internet facing systems and applications will be protected utilizing a layered approach to security controls.
 - 5.2.3.1 Remote access to the University information technology resources shall be permitted only through ITS approved remote access methods.
 - 5.2.3.2 Secure coding practices must be established and enforced for all application development.
 - 5.2.4 The use of cloud-based service providers shall be assessed for use. Product vendors are required to provide appropriate assurance of their security measures.

- 5.2.5 Physical access to core IT devices must be secured such that only those requiring physical access to the devices as part of their normal employment function are granted physical access.
- 5.2.6 Automated malware detection, prevention and correction mechanisms shall be operated, monitored and maintained on all University endpoints.
- 5.2.7 The University's electronic information must be disposed of in accordance with the *Records Retention and Destruction Procedure*.

6.0 ASSOCIATED PROCEDURES

None

7.0 RELATED POLICIES, FORMS, AND OTHER DOCUMENTS

- Privacy Policy
- Records Retention and Destruction Procedure
- Internal standards and procedures in ITS
- Data Classification Standard

8.0 ACCOUNTABILITY

Policy Sponsor

Vice-President, Finance and Administration & CFO

Responsible Office

Information and Technology Services

9.0 HISTORY

Relevant Dates

Approved: **25.10.01**
Effective: **25.10.01**
Next Review: **30.10**

Modification History

- 15.04.23:** New policy developed as part of an institutional Information and Technology Management (ITM) Control Framework. The overall framework establishes the control environment for the governance, management, and security for the university systems and data. This policy focuses on protecting personal and business information and implementing a system of identity management for the university. Approved by Board Motion 01-04-23-2014/15.
- 25.10.01:** Comprehensively revised to ensure alignment with current operational practices. Formerly titled Information Security and Identity Management. Approved by Audit and Risk Committee of the Board of Governors Motion ARC#-01-10-01-2025/26.