1.0 POLICY STATEMENT:

As a publicly-funded organization whose core business activities and service-delivery model are heavily reliant on personal and business information, MacEwan University ("University") accepts the critical responsibilities of securing information collection, usage and retention tools that are technology-dependent, protecting personal and business information and implementing a system of identity management.

2.0 RATIONALE AND GUIDING PRINCIPLES:

Information is a valuable asset that is at the core of, and enables, student learning and the University's academic and administrative processes. Information and related technology will be managed through privacy, security and identity management structures and processes that:

- Comply with legislation, regulations, contractual requirements and internal policies;
- Use privacy, security and identity management structures and processes to conceive, design, build and maintain information systems;
- Manage information throughout its lifecycle in accordance with its value, criticality, and requirement for confidentiality;
- Maintain trust between the University and its information users;
- Uphold information subjects' rights by obtaining informed consent when required;
- Provide access to information based on the principles of least-privilege, need-to-have and need-to-know;
- Achieve the academic and administrative goals of information use by meeting information quality criteria of confidentiality, integrity and availability;
- Ensure activities and decisions related to information security are open, transparent, and understandable.

3.0 SCOPE AND DEFINITIONS:

3.1 Scope

This policy applies to all information and related technology in the custody or control of the University, regardless of media. Privacy, security and identity management controls will be proportionate to the content or subject matter, sensitivity of the information and the assessed risk.

3.2 Definitions

3.2.1 "Compliance" means the University's responsibility to operate in agreement with established laws, regulations, standards, and specifications both internal and external.

3.2.2 "Control" means the policies, standards, procedures, practices and organizational structures designed to provide reasonable assurance that academic and administrative objectives will be achieved and undesired events will be prevented or detected and corrected.

3.2.3 "Information Quality Criteria" means the core criteria of confidentiality, integrity and availability.

3.2.4 “Least-Privilege” means the practice of limiting access to the minimal level that will allow normal functioning. Applied to employees, least-privilege means giving people the least amount of system privileges that would allow them to perform their job duties.

3.2.5 “Officer” means the president, vice presidents and equivalent positions, deans, directors and equivalent positions.

3.2.6 "Segregation of Duty ("SoD")" means that no employee or group of employees should be in a position both to perpetrate and to conceal errors or fraud in the normal course of their duties. In general, the principal incompatible duties to be segregated are:

3.2.6.1 Custody of assets.

3.2.6.2 Authorization or approval of related transactions affecting those assets.

3.2.6.3 Recording or reporting of related transactions.

3.2.7 "Standard" means a mandatory requirement, code of practice or specification established and approved by authority that is used as a baseline to measure the quality or performance of a process or procedure.

4.0 REGULATION:

4.1 The University will protect its information and related information technology assets from unauthorized access, use, disclosure, disruption, modification, or destruction in conformance with the principles and requirements set out in the *Information Security Framework Standard*.

4.2 The University will manage roles, responsibilities, access privileges and levels of authority in conformance with the requirements set out in the *Role Design Standard.*

4.3 The University will define, justify and maintain adequate SoD for business processes in conformance with the requirements set out in the *Segregation of Duties Standard.*

4.4 The Office of the Chief Information Officer will:

4.4.1 Maintain standards and procedures in relation to the governance and management of the University's information and related technology assets;

4.4.2 Advise Officers regarding continuance of or amendments to such standards and procedures as may be required.

FACT SHEET

Relevant Dates:

Dates:

Approval	2015.04.23
Review date	2020.04

Source:

2015-04-23	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.

Authorization:

Office of Accountability:	IT Compliance and Information Security
Office of Administrative Responsibility:	IT Compliance and Information Security
Approved By:	ITM Committee Board of Governors
Contact Area:	Office of the Chief Information Officer

Related and Associated Matters

Related Policies and Standards:
D8040 Enterprise Architecture
D8000 ITM Governance and Management
D8020 Information Management
D8030 Technology Management
D7500 Privacy

Associated Standards:
D8010-1 Information Security Framework Standard
D8010-2 Role Design Standard
D8010-3 Segregation of Duties Standard