1.0 POLICY STATEMENT

1.1 The purpose of this policy is to ensure the secure and responsible use of MacEwan University's ("University") Information Technology Resources. These requirements are designed to protect both the individual users and the University from a range of technological risks, including cybersecurity threats, privacy breaches, and non-compliance with legal and regulatory requirements. Inappropriate use of computing resources can compromise confidentiality, integrity, and availability of university systems, data, and services, hindering the University's ability to achieve its institutional objectives.

2.0 PURPOSE

2.1 This policy promotes a defense-in-depth approach to information security, requiring layered safeguards and ongoing monitoring to assess the effectiveness of security controls. It also supports the University's compliance with internal policies, applicable legislation, and regulatory obligations.

3.0 APPLICABILITY

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

4.0 DEFINITIONS

IT Resources
All University owned or managed Information Technology(IT) assets or services used to communicate, create, disseminate, store, and manage electronic information for academic, administrative, research, and operational activities.

Members of the MacEwan University Community
A person engaged in, or associated with, the conduct of University affairs, including but not limited to students, employees, suppliers, contractors, and visitors, while on University premises or in the use of University property.

Personal Information
Recorded information about an identifiable individual as defined under the *Access to Information Act* and the *Protection of Privacy Act*, which includes but is not limited to an individual's name, age, ID number, ethnic origin, educational, employment, financial, biometric information, medical history, or an opinion about the individual.

Remote Work
An approved work arrangement in which employees perform their job responsibilities from a location outside the organization's premises and uses secure technologies in compliance with the Information Security Policy to access corporate systems, data, and communication tools.

Technology Support
The team in Information Technology Services (ITS) that supports the Members of the MacEwan University Community and IT Resources.

Managed Device
Any computing device that is owned, maintained or provisioned by Technology Support and subject to University security and usage policies.

University Data
Data or information created or developed through academic, research, or administrative activities may be subject to ownership rights depending on applicable policies, agreements, or legislation.

Users
Any Member of the MacEwan University Community who has any level of access to IT Resources.

Virtual Private Network (VPN)
A secure network connection that allows Users to access internal resources remotely while ensuring confidentiality, integrity, and authenticity through encryption and secure tunneling protocols.

5.0 POLICY ELEMENTS

5.1 General

5.1.2 The University provides IT Resources to Users to to support the effective operation of the insititution and the delivery of academic and administrative services.

5.1.2.1 Application and enforcement of this policy shall not in any way constrain academic freedom on campus.

5.1.3 Using IT Resources for commercial or financial profit, unless explicitly authorized in writing by the University, is strictly prohibited.

5.1.4 The IT Resources must not be used to create, transmit, store, access, or view material that contributes to, supports, or promotes harassment or discrimination in any form, except where such use is explicitly authorized as part of approved academic, research, or investigative activities.

5.1.4.1 This includes, but is not limited to, content involving sexual and gender-based violence, pornography, racial, ethnic, or cultural harassment, hate literature, systemic discrimination, or any other material prohibited under University policies on harassment, discrimination, and reprisal.

5.1.5 Users must not share account credentials, impersonate others, or conceal their identity. Users are responsible for all activities conducted under their assigned user identity when using IT Resources.

5.2 Privacy

5.2.1 The University recognizes the importance of maintaining reasonable privacy for electronic files stored or transmitted via its networks, however, users should not expect complete privacy when utilizing IT Resources, as these systems may be subject to monitoring and access in accordance with institutional policies and applicable laws.

5.2.2 IT Resources are subject to monitoring under the University's custodianship. Monitoring may include, but is not limited to:

- During the normal course of managing and administering IT Resources.
- During the investigation phase of an information security incident.
- As necessary for law enforcement or litigious purposes, or with the approval of an officer of the University, where allegations of inappropriate use are suspected.

5.2.3 Monitoring may also be conducted to support Human Resources workplace investigations, employee relations matters, or other employment-related inquiries, with authorization from appropriate University leadership.

5.3 Remote Work & Bring Your Own Device ("BYOD")

5.3.1 The University supports remote work where operationally appropriate. VPN access is provisioned based on business need and must be used in accordance with the University access policies. Remote access from outside the country requires prior authorization and must comply with applicable information security standards.

5.3.2 Users working on files off-campus must use the preferred method to access University Data through approved cloud file services.

5.3.3 The University permits the use of BYOD for University purposes, provided that Users comply with University policies and procedures for data handling and security.

5.3.4 Any records created, stored, or transmitted on a BYOD in the course of conducting University business may be deemed to be under its custody or control. As such, these records are subject to authorized investigations, audits or reviews in accordance with applicable legislation and policies.

5.3.5 Users are expected to maintain a reasonable level of device hygiene when working remotely on personally owned devices. This includes keeping operating systems and software up to date, using endpoint protection, and ensuring that devices are protected by strong authentication. While not all controls can be enforced on personal devices, failure to follow safe computing practices may result in the revocation of remote or BYOD access privileges.

5.3.6 Software licensed to the University must not be installed on personally owned devices unless permitted by the licence terms or authorized by Information Technology Service.

5.4 Managed Devices

5.4.1 Users are prohibited from performing the following actions on Managed Devices:

5.4.1.1 Altering, disabling, bypassing, or interfering with security tools or configurations deployed by the University.

5.4.1.2 Storing or accessing unauthorized music, videos, or other copyrighted materials via peer-to-peer file sharing on University computers, network or cloud storage systems.

5.4.1.3 Leaving Managed Devices unattended while logged in. Managed Devices must be locked or logged out to prevent unauthorized access.

5.4.1.4 Inserting unintended or unknown removable media into any Managed Device. Such media should be promptly reported to Technology Support for appropriate handling.

5.4.2 Users are responsible for the physical security of their issued Managed Device.

5.4.3 Data stored on Managed Devices, whether personal or University Data, is governed by the University's data protection rules. Personal privacy is not guaranteed as the University is responsible for safeguarding data in accordance with its security and privacy obligations.

5.4.4 A Managed Device suspected to be missing or stolen must be reported immediately to campus security and Technology Support.

5.5 Network & Internet

5.5.1 Guest Users must comply with the University *Guest Wireless Standard* when accessing the University's wireless network.

5.5.2 Users are prohibited from engaging in the following activities, including but not limited to:

5.5.2.1 Modifying network settings or configurations to gain unauthorized access to computer systems, services, or data.

5.5.2.2 The use of network inspection, security scans, or packet capture technologies unless explicitly authorized by the Director, Cyber Security & Chief Information Security Officer or their designate.

5.5.2.3 Circumventing authentication controls or compromising the security of any host, network, or account.

5.5.2.4 Connecting unapproved networking equipment such as routers, switches or wireless access points to any part of the University network.

5.5.2.5 Accessing or attempting to access network or system configuration information for which the user does not have administrative rights.

5.5.2.6 Engaging in activities that deliberately consume excessive network bandwidth, interfere with network performance, or disrupt access to legitimate services.

5.5.2.7 Access to websites that threaten network security, create legal risk, harm the University's reputation, or violate institutional policies.

5.5.3 Websites deemed to be malicious to the University network will be automatically blocked.

5.6 Electronic Communications

5.6.1 All electronic communications must adhere to University standards for privacy, security, and data protection, ensuring sensitive and personally identifiable information is encrypted and handled with appropriate safeguards.

5.6.2 Sending unsolicited email messages, including the sending of "junk mail", "chain letters", political statements, or other advertising material to anyone who did not specifically request such material is prohibited and may be in violation of the Canadian Anti-Spam Legislation.

5.6.3 E-mail and instant messaging must be professional, appropriate, and consistent with applicable University policies. Communications must not include content that could be considered offensive, discriminatory, or damaging to the University's reputation.

5.6.4 When using a University email address outside of official University business, the User must ensure its use does not imply endorsement by the University.

5.6.5 Users are solely responsible for the content they disseminate. The University is not responsible for any third-party claim, demand, or damage arising from the misuse of the IT Resources.

5.6.6 University Data must not be transmitted to personal email accounts or copied to personal storage devices, such as flash drives, for access outside the University's authorized computing environment, unless explicitly permitted by institutional policy and in compliance with applicable privacy regulations.

5.6.7 University business must be conducted using approved accounts or identity and not personal email or public instant messaging platforms except where prior authorization has been granted by the University for specific circumstances.

5.6.8 The exchange of user credentials, confidential information, or personal data via instant messaging platforms should be limited to transitory, time-sensitive situations. Such information must be managed appropriately in accordance with University policies and shared only with authorized individuals. Where possible, secure email should be used as the preferred method for transmitting sensitive information.

5.7 Artificial Intelligence

5.7.1 Users must adhere to University's policies, frameworks and guidelines on Artificial Intelligence.

5.8 Compliance & Reporting

5.8.1 By using the IT Resources, Users acknowledge and agree to comply with this policy.

5.8.2 Information Technology Services (ITS) in collaboration with Human Resources and the Office of General Council reserve the right to revoke, restrict, or limit access to IT Resources if there are reasonable grounds to suspect that the User continued access to the computing environment does not comply with this policy or poses a threat to the operation of the IT Resources or the reputation of the University.

5.8.3 Users must promptly report any known or suspected misuse of IT Resources or violations of this policy to Technology Support. Reports will be handled in accordance with and protected under, the Safe Disclosure Policy

6.0 ASSOCIATED PROCEDURES

None

7.0 RELATED POLICIES, FORMS, AND OTHER DOCUMENTS

- Artificial Intelligence Policy
- Information Security Policy
- Safe Disclosure Policy

- *AI Best Practices Guidelines*, Office of General Counsel
- *Artificial Intelligence – Student Guide,* MacEwan Library
- *Generative Artificial Intelligence in Your Class*, MacEwan Centre for Teaching and Learning
- Records Retention and Destruction Procedure
- Managing Personal Information Procedure
- Password Management Standard

8.0 ACCOUNTABILITY

Policy Sponsor
Vice-President Finance and Administration & CFO

Responsible Office
Information and Technology Services

9.0 HISTORY

Relevant Dates

Approved:	**25.12.18**
Effective:	**25.12.18**
Next Review:	**30.12**

Modification History

25.12.18: New Policy. Approved by Board of Governors motion #BOG-02-12-18-2025/26.