1.0 ASSOCIATED POLICY

- ITM Governance and Management Policy

2.0 DEFINITIONS

Credentials
Credentials include usernames, access codes, account numbers, passwords, PINs, electronic signatures, and tokens which may have been assigned to users who are authorized to access University information technology resources.

Electronic Signatures
A university-approved electronic method of marking an electronic record that confirms the identity of the person who intended to sign the record, confirms the intention to sign the record, and preserves the integrity of the record once it has been signed.

Information technology resources
Information technology resources refer to all hardware, software, and supporting infrastructure owned or managed by, or in the custody of, the University that are used to create, retrieve, manipulate, transfer, and store electronic information. This includes, but is not limited to, computers, software, wired and wireless networks, telecommunication and portable devices, cloud services, social media channels and data stored on, or in transit, on the above.

Official social media channels
All social media accounts established on behalf of the university and its business and academic units.

Social media
Online communication channels dedicated to community-based input, interaction, content-sharing and collaboration.

System and network administrators
System and network administrators refer to persons responsible for configuring, installing, maintaining, and supporting information technology resources for the University. A system or network administrator of an information technology resource may also be a user of that resource.

Users
Everyone who uses the information technology resources owned or managed by the University.

3.0 PROCEDURE ELEMENTS

3.1 Overview

MacEwan University (the "University") strives to create and maintain an intellectual environment in which students, faculty, and staff feel free to create and to collaborate with colleagues at the University without fear that the products of their intellectual efforts will be violated, misrepresented, tampered with, destroyed, or stolen. This intellectual environment is fostered by an atmosphere of trust and confidentiality that, in part, is supported by the information technology resources made available to the University community.

3.2 Scope

The University works to maintain information technology resources that are readily accessible to its users and requires that their use be in a manner that is secure, responsible, ethical, respectful, and free from harassment. The use of these resources must, therefore, be in accordance with policy and regulation established from time to time by the University and its operating units.

3.3 Requirements

3.3.1 University information technology resources must be used in a manner that is secure, responsible, ethical and respectful. Use of these resources for disruptive, discriminatory, illegal, harassing or malicious purposes is strictly prohibited.

3.3.2 University information technology resources must be used primarily for activities related to the mission of the University, including, but not limited to teaching, learning, research, and administration.

3.3.3 Incidental personal use of information technology resources, i.e. use not related to the mission of the University, is permitted provided it complies with this standard, does not compromise the business of the University, does not increase the University's costs, does not expose the University to additional risk, and does not damage the University's reputation or brand.

3.3.4 Users are responsible for any activity originating from their University-provisioned accounts which they can reasonably be expected to control.

3.3.5 Use of information technology resources to create, transmit, or receive information owned by, or in the custody or under the control of, the University must protect that information in a manner that is commensurate with its value, use, and sensitivity.

3.3.6 Users will comply with all copyright and licensing agreements. The University will assist any copyright owner, with just cause, to notify individuals violating copyright laws.

3.3.7 Users shall not attempt to circumvent data protection schemes or uncover security vulnerabilities.

3.3.8 Users shall not attempt to degrade system performance or capability, or attempt to damage systems, software, or intellectual property of others.

3.3.9 Accounts and passwords or other credentials that are used for authentication may not, under any circumstances, be used by persons other than those to whom they have been assigned by the University.

3.3.10 Users may use their credentials to electronically sign documents or approve transactions. Such transactions shall have the same status as a handwritten signature.

3.3.11 Only information technology resources that rely on University authentication services are allowed and deemed as reliable electronic signatures. Users shall not sign an electronic record except by using the electronic signature service(s) approved for use by the University.

3.3.12 Users shall not use the University information technology resources to gain unauthorized access to university and external computer systems or services.

3.3.13 Users shall not attempt to monitor another user's data communications.

3.3.14 Use of Information technology resources and data that is owned by, in the custody of or under the control of the University for personal profit or non-university commercial gain is prohibited.

3.3.15 Information and Technology Services monitors and logs the usage of information technology resources.

3.3.15.a Information and Technology Services will withhold or revoke access to information technology resources if there are reasonable grounds to suspect that continued access poses a threat to the operation of information technology resources or to the reputation of the University.

3.3.15.b Information and Technology Services has the right to access both stored or in-transit data when there is suspected or alleged impropriety, a business need for access in the absence of an employee, a request under the Freedom of Information and Protection of Privacy Act, or as otherwise required by law. This information will be used in disciplinary action as deemed appropriate and in accordance with employment policies, collective agreements, and/or policy E3102 Student Discipline, as applicable, and provided to appropriate internal and external investigative authorities.

3.3.15.c Nothing in this Standard precludes system and network administrators from taking action in the case of suspected abuse of information technology resources. System and network administrators will take immediate action when the University is at imminent risk.

3.4 Compliance and Exceptions

Responsibility for compliance with MacEwan policies and standards extends to all students, faculty, staff, and all individuals or entities using any MacEwan IT resource and all use of such resources. Violations of this standard may result in the revocation or limitation of IT resource privileges.

Compliance with the requirements of this standard will be enforced by the IT Compliance and Information Security Office.

3.5 Measurement

The following measurements will be used to monitor the overall effectiveness of the Use of Information Technology Resources Standard.

3.5.1 Number of incidents where information technology resources were used in a manner that was threatening or harassing.
3.5.2 Number of instances when users attempted to circumvent security configurations and uncover security vulnerabilities.
3.5.3 Number of suspensions of accounts.

4.0 RELATED POLICIES, PROCEDURES, FORMS AND OTHER DOCUMENTS

- Information Security and Identity Management Policy
- Privacy Policy

8.0 ACCOUNTABILITY

Policy Sponsor
Vice-President, Resources and People

Responsible Office
Office of the AVP Information Services and Chief Information Officer

9.0	HISTORY
Relevant Dates	
Approved:	**20.07.14**
Effective:	**20.07.14**
Next Review:	**23.07**
Modification History	
17.04.12:	Standard approved.
20.07.14:	Revised to define and allow the use of electronic signatures. Approved by the President's Policy Committee.