



Use of Information Technology Resources

Standard D8000-7

Effective Date: April 27, 2017

Authority & Alignment

Authority and Alignment: MacEwan University Employee Code of Conduct, D3300 Internal Controls, D8000 ITM Governance and Management

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.

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.

Scope and Definitions

This standard applies to everyone who uses the information technology resources owned or managed by the University including, but not limited to, data, information, hardware, software, the network and official social media channels.

1. **Credentials.** Credentials include usernames, access codes, account numbers, passwords, PINs, and tokens which may have been assigned to users who are authorized to access University information technology resources.
2. **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.
3. **Official social media channels.** All social media accounts established on behalf of the university and its business and academic units.

4. **Social Media.** Online communication channels dedicated to community-based input, interaction, content-sharing and collaboration.
5. **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.
6. **Users.** Everyone who uses the information technology resources owned or managed by the University.

Compliance & Exceptions

Responsibility for compliance with MacEwan policies and standards extends to all members of the MacEwan community. Non-compliance may create risk for MacEwan and will be addressed accordingly.

Standard Requirements

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.
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. 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.
4. Users are responsible for any activity originating from their University-provisioned accounts which they can reasonably be expected to control.
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.
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.
7. Users shall not attempt to circumvent data protection schemes or uncover security vulnerabilities.
8. Users shall not attempt to degrade system performance or capability, or attempt to damage systems, software, or intellectual property of others.
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.
10. Users shall not use the University information technology resources to gain unauthorized access to university and external computer systems or services.

11. Users shall not attempt to monitor another user's data communications.
12. 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.
13. Information and Technology Services monitors and logs the usage of information technology resources.
 - 13.1. 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.
 - 13.2. 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.
 - 13.3. 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.

Related Content	
Type	Title
Policy	D8000 Information and Technology Management Policy
Policy	D1125 Harassment Policy
Policy	D7500 Privacy Policy
Policy	E3101 Student Rights and Responsibilities
Standard	D8030-3 Manage Third Party Services

Measurement

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

Contact

Chief Information Officer