MISERICORDIA UNIVERSITY

Origination: *09/2021*
Effective: *09/2021*
Last Approved: *09/2021*
Policy Steward: *Mark Reboli: Networking and Telecommunications Manager*
Area: *IT, Networking Group*

Acceptable Use of Information Technology Resources Policy

I. Reason for the Policy

To ensure all users of information technology (IT) resources understand their role(s) and responsibilities when utilizing university information technology resources.

II. Policy Statement

Appropriate university use of information and information technology ("IT") resources and effective security of those resources require the participation and support of the university's workforce, students and affiliates ("users"). Inappropriate use exposes the university to potential risks including virus attacks, compromise of network systems and services, and legal issues.

III. Who Should Read This Policy

This policy applies to users of any system's information or physical infrastructure regardless of its form or format, created or used to support the university. It is the user's responsibility to read and understand this policy and to conduct their activities in accordance with its terms.

IV. The Policy

Except for any privilege or confidentiality recognized by law, individuals have no legitimate expectation of privacy during any use of the university's IT resources or in any data on those resources. The data and use maybe accessible via automated reporting tools (Intrusion Detection System (IDS), Antispam/Antivirus systems etc.) reporting programs and tools (meant to monitor the health and security of the network/systems), via the course of normal IT operations (bandwidth studies, address pc problems) or via Human Resources or Vice President approvals when warranted. Users may also be notified with a warning banner text at system entry points where users initially sign on about the use or unauthorized access of the university's IT resources is not permissible.

The university may impose restrictions, at the discretion of their executive management, on the use of a particular IT resource. For example, the university may block access to certain websites or services not serving legitimate business purposes or may restrict user ability to attach devices to the university's IT resources (e.g., network devices).

1. Acceptable Use

All uses of information and information technology resources must comply with university policies, standards, procedures, and guidelines, as well as any applicable license agreements and laws including Federal, State, local and intellectual property laws.

Consistent with the foregoing, the acceptable use of information and IT resources encompasses the following duties:

- Understanding the baseline information security controls necessary to protect the confidentiality, integrity, and availability of information;
- Protecting university information and resources from unauthorized use or disclosure;
- Protecting personal, private, sensitive, or confidential information from unauthorized use or disclosure;
- Ensuring the use of resources in the proper manner to protect against phishing attacks
- Observing authorized levels of access and utilizing only approved IT technology devices or services; and
- Immediately reporting suspected information security incidents or weaknesses to the appropriate manager and the Information Security Officer (ISO)/designated security representative.

2. Unacceptable Use

The following list is not intended to be exhaustive but is an attempt to provide a framework for activities that constitute unacceptable use. Users, however, may be exempted from one or more of these restrictions during their authorized job responsibilities, after approval from university senior management, in consultation with university IT staff (e.g., storage of objectionable material in the context of a disciplinary matter). Unacceptable use includes, but is not limited to, the following:

- Unauthorized use or disclosure of personal, private, sensitive, and/or confidential information;
- Unauthorized use or disclosure of university information and resources;
- Distributing, transmitting, posting, or storing any electronic communications, material or correspondence that is threatening, obscene, harassing, pornographic, offensive, defamatory, discriminatory, inflammatory, illegal, or intentionally false or inaccurate;
- Attempting to represent the university in matters unrelated to official authorized job duties or responsibilities;
- Connecting unapproved devices to the university's network or any IT resource;
- Connecting university IT resources to unauthorized networks;
- Connecting to any wireless network while physically connected to the university's wired network;
- Installing, downloading, or running software that has not been approved following appropriate security, legal, and/or IT review in accordance with university policies;
- Using a university's IT resources to circulate unauthorized solicitations or advertisements for non-university purposes including religious, political, or not-for-profit entities;
- Providing unauthorized third parties, including family and friends, access to the university's IT information, resources or facilities;
- Using university IT information or resources for commercial or personal purposes, in support of "for-profit" activities or in support of other outside employment or business activity (e.g., consulting for pay, business transactions);
- Propagating chain letters, fraudulent mass mailings, spam, or other types of undesirable and unwanted email content using university IT resources; and
- Tampering, disengaging, or otherwise circumventing a university or third-party IT security controls.

3. Occasional and Incidental Personal Use

Occasional, incidental and necessary personal use of IT resources is permitted, provided such use: is otherwise consistent with this policy; is limited in amount and duration; and does not impede the ability of the individual or other users to fulfill the university's responsibilities and duties, including but not limited to, extensive bandwidth, resource, or storage utilization. Exercising good judgment regarding occasional and incidental personal use is important. The university may revoke or limit this privilege at any time.

4. Individual Accountability

Individual accountability is required when accessing all IT resources and university information. Everyone is responsible for protecting against unauthorized activities performed under their user ID. This includes locking your computer screen when you walk away from your system, and protecting your credentials (e.g., passwords, tokens, or similar technology) from unauthorized disclosure. Credentials must be treated as confidential information and must not be disclosed or shared.

5. Restrictions on Off-Site Transmission and Storage of Information

Users must not transmit restricted university, non-public, personal, private, sensitive, or confidential information to or from personal email accounts (e.g., Gmail, Hotmail, Yahoo) or use a personal email account to conduct the university's business unless explicitly authorized. Users must not store restricted university, non-public, personal, private, sensitive, or confidential information on a non-university issued device, or with a third-party file storage service that has not been approved for such storage by the university.

Devices that contain university information must be attended at all times or physically secured and must not be checked in transportation carrier luggage systems.

6. User Responsibility for IT Equipment

Users are routinely assigned or given access to IT equipment in connection with their official duties. This equipment belongs to the university and must be immediately returned upon request or at the time an employee is separated from the university. Users may be financially responsible for the value of equipment assigned to their care if it is not returned to the university. Should IT equipment be lost, stolen or destroyed, users are required to provide a written report of the circumstances surrounding the incident. Users may be subject to disciplinary action which may include repayment of the replacement value of the equipment. The university has the discretion to not issue or re-issue IT devices and equipment to users who repeatedly lose or damage IT equipment.

7. Use of Social Media

The use of public social media is governed by the Misericordia University Social Media Policy.

V. Definitions

VI. Procedures

Attachments

No Attachments

Approval Signatures

Step Description	Approver	Date
Final Approval	Daniel Myers: President	09/2021
Final Review	Mark Van Etten: Vice President, Finance and Administration	09/2021
	Val Apanovich: Director of Information Technology	09/2021
	Mark Reboli: Networking and Telecommunications Manager	09/2021