



**MISERICORDIA
UNIVERSITY**

Origination 09/2021
Last Approved 08/2025
Effective 08/2025

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 information technology (IT) resource users understand their role(s) and responsibilities when utilizing university IT resources.

II. Policy Statement

Appropriate use of information and IT resources and adequate security requires the participation and support of the University's workforce, students and affiliates ("users"). Inappropriate use can expose the University to risks, including virus attacks, system and service compromises, and legal issues.

III. Who Should Read This Policy

This policy applies to all users of any system's information or physical infrastructure created or used to support the University, regardless of form or format. Users are responsible for reading, understanding, and adhering to this policy.

IV. The Policy

Except where the law recognizes privacy or confidentiality, individuals should not expect privacy when using the University's IT resources or accessing data on those resources. Data and usage may be monitored through automated tools (e.g., Intrusion Detection Systems, Antivirus systems) and routine IT operations (e.g., bandwidth studies, addressing PC issues) or through Human Resources or Vice President approvals when warranted. Users may also receive warnings about unauthorized access through system entry banners.

At its discretion, the University may impose restrictions on IT resource use, including blocking access to

certain websites or services that do not serve legitimate business purposes or restricting the attachment of devices to the University's IT resources.

1. Acceptable Use

All use of information and IT resources must comply with university policies, standards, procedures, guidelines, and applicable laws, including federal, state, local and intellectual property laws. Acceptable use includes:

- Understanding baseline information security controls to protect the confidentiality, integrity, and availability of information.
- Protecting university information and resources from unauthorized use or disclosure.
- Safeguarding personal, private, sensitive, or confidential information.
- Ensuring proper use of resources to protect against phishing attacks.
- Adhering to authorized access levels and using only approved IT technology.
- Reporting suspected security incidents or weaknesses to the appropriate manager, IT Network Security Manager, or designated security representative.

2. Unacceptable Use

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 is prohibited.
- Distributing, transmitting, posting, or storing electronic communications or materials that are threatening, obscene, harassing, pornographic, offensive, defamatory, discriminatory, inflammatory, illegal, or intentionally false or inaccurate.
- Misrepresenting the University in non-official matters.
- Connecting unapproved devices to the University's network or any IT resources.
- Connecting university IT resources to unauthorized networks.
- Using university IT resources for unauthorized solicitations or advertisements.
- Providing unauthorized access to university IT resources to third parties.
- Using university IT resources for commercial or personal purposes, including outside employment or business activities.
- Propagating spam, chain letters, fraudulent mass mailings, or other unwanted email content is prohibited.
- Tampering with or circumventing IT security controls.

3. Occasional and Incidental Personal Use

Occasional, incidental, and necessary personal use of IT resources is permitted, provided it:

- It is consistent with this policy.
- It is limited in amount and duration.
- Does not impede the individual's or other's ability to fulfill university responsibilities, including extensive bandwidth or storage use.

The University may revoke or limit this privilege at any time.

4. Individual Accountability

Users are accountable for activities performed under their user IDs. Responsibilities include locking screens and protecting credentials (e.g., passwords, tokens) against unauthorized disclosure. Credentials must be treated as confidential information and not 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 via personal email accounts (e.g., Gmail, Yahoo) or use a personal email account for university business unless explicitly authorized. Users must not store information on non-university devices or unauthorized third-party storage services.

Users must ensure that devices containing university information are always physically secured and not checked in transportation carrier luggage systems.

6. User Responsibility for IT Equipment

Users are assigned or given access to IT equipment for official duties. This equipment remains university property and must return to the University upon request or upon employment separation. Users may be financially responsible for unreturned equipment. Lost, stolen or destroyed equipment must be reported in writing. Repeated loss or damage may result in disciplinary action or denial of future equipment issuance.

7. Use of Social Media

The Misericordia University Social Media Policy governs the use of public social media.

V. Definitions

VI. Procedures

Approval Signatures

Step Description	Approver	Date
Final Approval	Daniel Myers: President	08/2025
Final Review	Mark Van Etten: Vice President, Finance and Administration	08/2025
	David Johndrow jr: Director of Information Technology	05/2025
	Mark Reboli: Networking and Telecommunications Manager	05/2025

COPY