



**MISERICORDIA
UNIVERSITY**

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

Policy Steward Mark Reboli:
Networking and Telecommunications Manager
Area IT, Networking Group

Information Technology Resources Policy

I. Reason for the Policy

Misericordia recognizes the importance of IT resources supporting student learning, administrative functions, and communication. This policy guides the appropriate use of IT resources.

II. Policy Statement

Users must act responsibly, ethically, and legally when using Misericordia's IT resources, ensuring university data and systems' confidentiality, integrity, and availability.

III. Who Should Read This Policy

The policy applies to all users of IT resources, including employees, students, and contract workers.

IV. The Policy

Users are responsible for their actions and the resources entrusted to them. Users should use resources for university purposes, and confidential information must be protected.

Misericordia follows key IT security principles to support users maintaining confidentiality, integrity, and availability of data and services. Sensitive information must be treated as confidential unless otherwise classified. Users are also responsible for maintaining the integrity of physical facilities, licenses, and contracts. No user shall disrupt IT resources, limiting availability for others.

Users may "Choose Your Own Device (CYOD)" to a limited extent for official duties, but university-owned devices must be used whenever possible due to their advanced security protections. Users should not store sensitive or confidential information on personal devices.

The privilege of access to university IT resources is to students, employees, and affiliates. The University reserves the right to deny access to those outside the community. System administrators are entrusted

with maintaining the security of information resources and may take necessary actions to ensure this.

1. Access to Information Resources:

University IT resources are for academic and University purposes. Incidental personal use is permissible, provided it does not consume significant resources or interfere with university operations. Students may use the student network for entertainment, following university policies such as:

- Acceptable Use of Information Technology Resources Policy
- Peer-to-Peer Policy
- Compliance with state and federal laws

Affiliates may access IT resources with sponsorship from a full-time employee in consultation with the IT Network Security Manager. Utilization of IT resources for personal profit is prohibited.

Misericordia is not liable for unauthorized access or technology failures, including service interruptions due to security measures.

2. User Responsibilities:

Users must uphold information security principles (confidentiality, integrity, availability) and follow best practices in IT hygiene, including:

a. Information Technology Resource Hygiene

Good computer hygiene involves practices that maintain system health and improve online security, including:

- Ensuring an active, updated antivirus and anti-malware program.
- Updating operating systems, device drivers, and applications regularly.
- Enabling an active personal firewall.
- Enabling password-protected screen savers after 15 minutes of inactivity.
- Conducting weekly virus and malware scans.

b. Information Technology Account Hygiene

Users must secure their accounts through practices such as:

- Using strong, secure passwords with multi-factor authentication.
- Reporting compromised accounts immediately.
- Changing passwords at least annually and log in at least every six months.
- Using only personal account(s) assigned.
- Participating in required annual security awareness training.

c. Internet Hygiene

Users provided with Internet access must comply with university policies, including:

- Being responsible for the content shared online.
- Refraining from sending anonymous communications.
- Avoiding downloading unauthorized software or visiting risky websites.
- Understanding Internet usage may be monitored.

d. Physical Security and Responsibilities

Users must safeguard university-owned equipment, including:

- Protecting equipment from theft or damage.
- Carrying university devices as carry-on baggage when traveling.
- Reporting equipment losses immediately to the PC Services Manager or Director of IT.
- Returning unneeded IT resources for secure disposal or reallocation.
- Not loaning equipment to non-university personnel unless authorized.

e. Proactive Responsibilities to Improve Security

Users should:

- Backup important data to approved storage.
- Encrypt sensitive information.
- Avoid downloading university confidential data to unencrypted portable devices.
- Only use licensed software on university equipment.
- Avoid storing personal information on university equipment.

f. Reporting issues and System Documentation

Report technology issues and document system irregularities or security vulnerabilities immediately.

g. Circumventing Security

Users play a pivotal role in cybersecurity, reporting any issues, compromises, or vulnerabilities they identify. Below are actions that are strictly prohibited:

- Users must not intentionally seek information, browse, obtain copies, or modify files or passwords belonging to others unless specifically authorized to do so.
- Users may not seek to add permissions or access for which they do not have a business reason.
- Users must refrain from any unauthorized actions that deliberately interfere with the operating systems or functions of systems.

- Users must not alter or change device configurations (hardware or software) on information resources provided to them.
- Users shall not use any information resource as a staging ground to enter other systems without authorization.
- Users shall not transfer University-owned programs and data to unauthorized sites.
- Users may not use programs obtained from commercial sources or other computer installations unless approved in advanced by either the PC Services Manager or Director of IT.
- Users must not attempt to circumvent data protection schemes or uncover security loopholes, including creating programs designed to identify vulnerabilities in decrypting secure data.

V. Definitions

Sensitive data (sensitive information) - Institutional information requiring protection due to proprietary, ethical, privacy, or business process concerns.

Confidential data (confidential information) - Institutional information protected by regulations, obligations, or specific university policies.

Production system - A system used to organize or automate office tasks or store information for departmental purposes.

VI. Procedures

COPY

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