MISERICORDIA UNIVERSITY

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

Information Technology Resources Policy

I. Reason for the Policy

Misericordia recognizes the value and sensitivity of computer and other electronic resources to improve student learning and to enhance the administration and operation of the university. To this end, Misericordia has provided guidance on responsibilities and appropriate use of computers; computer networks, including the Internet; and other electronic resources in support of the mission and goals of Misericordia.

II. Policy Statement

It is appropriate for all users to behave in a responsible, ethical and legal manner whenever utilizing Misericordia' s information technology resources. In general, appropriate use means respecting the rights of other users, and maintaining the critical tenets; confidentiality, integrity, and availability of all data/information (information) and resources at the university.

III. Who Should Read This Policy

The policy applies to all users who make use of Misericordia information technology resources. This policy also applies where the employee is not physically working in university-owned offices, and includes remote workers, part-time remote workers, and contract labor.

IV. The Policy

All users of university information resources are responsible for their actions and the actions of resources (accounts and devices) entrusted to them. All users should behave in a responsible way to ensure resources are utilized appropriately for university or educational pursuits.

Misericordia has determined to follow the three information technology security tenets in support of users utilizing information technology resources. Confidential information shall be maintained to the sensitivity level to which it is classified, when not appropriately classified, the information should be considered confidential until such time as it is appropriately classified to a lower level. The integrity of the physical facilities, all pertinent licenses, and contractual agreements, and ensuring the integrity of information is the responsibility of all users who interact with such. No user shall impact the information technology resources impeding the availability of the resources to others at the university.

All access to university information technology resources are a privilege granted by the university to students, employees, and affiliate members of the Misericordia community. The University reserves the right, in its sole

and absolute discretion, to refuse access to information technology resources at the university to anyone who is not a member of the university community.

The University vests the oversight responsibility for ensuring the confidentiality, integrity, and availability of its information resources in various system administrators. While respecting the rights of all users, when the tenets are threatened, administrators are authorized to take those actions necessary to maintain the confidentiality, integrity, and availability of the information technology resources.

1. Access to Information Resources:

Students, employees and affiliate members of the Misericordia community may have access to the information technology resources of the university as long as the user appropriately complies with this and other policies that govern the use of information technology resources (e.g., Acceptable Use of Information Technology Resources, etc.)

In general, the university information technology resources are intended to be used for university and educational purposes only. Incidental personal use is nonetheless permissible if the use does not consume more than a trivial amount of resources that could otherwise be used for business or educational purposes, does not interfere with employee productivity, does not preempt any business or educational activity, and does not cause distress, legal problems, or morale problems for other employees.

The university has established time-sharing computer facilities that may be used for activities related to research, instruction, or administrative purposes. Student may utilize the student network via their own device for entertainment purposes so as long as they comply with;

a. Compliance with this and other Misericordia policies, including but not limited to:
    i. Acceptable Use of Information Technology Resources Policy
    ii. Peer-to-Peer Policy
b. Compliance with all state, federal laws and acts
c. The use of such does not overburden the resources of the university.

The university at its sole and absolute discretion may provide access to affiliate members of the university. In such cases this access may be granted when sponsored and approved by a full-time employee in consultation with the IT Security Manager.

At no time may information technology resources be utilized for personal profit.

Misericordia is not liable nor is the information technology staff to be held accountable for unauthorized access by other users, nor can they guarantee protection against media failure, fire, or other disasters. Users may experience temporary denial of services at times due to technological failures, or via university employing tools to carryout responsibilities for which they are authorized to do so.

2. User Responsibilities:

A user of information technology resources at the university are required to ensure that the tenets of information security (confidentiality, integrity, availability) are supported and maintained. The user's responsibilities include but are not limited to the following:

a. Information Technology Resource Hygiene

Good computer hygiene refers to the basic practices and steps that users of computers and other devices take to maintain system health and improve online security. These practices are often part of a routine to ensure the safety of identity and other details that could be stolen or corrupted. These include:

- Ensure that an actively monitoring antivirus program is working and up to date.
- Ensure operating system, system device drivers, and applications are up to date.
- Ensure anti-malware software is active and up to date.
- Ensure an active personal firewall is enabled.
- Secure all PCs, laptops, workstations, and other devices with a password-protected screen saver with the automatic activation features set to 15 minutes' maximum.
- Scan the devices that the user is responsible for at least weekly to ensure that the resource(s) is up-to-date, virus free and malware free.

b. Information Technology Account Hygiene

Good account hygiene refers to the basic practices and steps that users can take secure their identity and access on systems, devices, and services controlled by their access credentials.

- Users are solely responsible for the account the user has been provided with.
- Users should set a password not guessed easily.
- Users are required to utilize multi-factor authentication (MFA)/2-Factor (2FA) on their accounts as activated by the IT Department especially when utilizing email.
- If a user discovers their password is compromised, it is the user's responsible to notify the Information Technology Security Manager or Director of Information Technology in writing immediately.
- Users must change their password at least annually.
- Users must only use account(s) that belong to the user.
- Users must participate in yearly security awareness training required by the University.
- Users must log into their accounts at least once in a 6-month window or their access shall be disabled.

c. Internet Hygiene

University employees, students, and affiliate members of the university community that have a legitimate university need are provided Internet access so as long as the user fully comply with university policies. Full compliance includes but is not limited to:

- Each user is responsible for the content of all text, audio, or images that the user places on sends over the university's Internet system.
- No electronic communication may be sent that hides the identity of the sender or represents the sender as someone else, or someone from another company.
- To prevent malware infection/spread through the university's Internet system, users should be extremely vigilant in downloading of any software, viewing any sites, or clicking on any links.
- The university monitors usage patterns in its Internet communications for various reasons, including cost analysis, security, bandwidth allocation, and general management of the university's gateway to the Internet. Users should therefore not assume electronic communication are totally private and should transmit sensitive (confidential) data in other ways.

d. Physical Security and Responsibilities

Physical Security and Responsibilities ensure good care of resources that end users have been provided with. These include:

- The safeguarding of all university owned equipment assigned to the user exclusive or shared use, all university equipment within the user's work areas from theft or physical damage.
  - For example, when the user travels with university owned equipment such as mobile computers, these devices must always be carry-on baggage not check-baggage.
  - Users must report any equipment losses immediately to the PC Services Manager or Director of Information Technology in writing, so that the Information technology department can assist in how to proceed.
- All information technology resources when no longer utilized for the requested university purposes shall be returned to the Information Technology Department for sanitization, secure disposal, or reallocation.
- Equipment shall not be loaned to non-university personnel. Additionally, equipment containing sensitive (confidential) information shall not be loaned to someone not authorized to all information stored on the device.

e. Proactive Responsibilities to Improve Security

Security and being proactive is everyone's responsibility. By performing these responsibilities, the university looks to lessen attack vectors and ensure that end-user information is secured.

- User must backup all locally created data to a university-approved storage area in case the portal device is lost, damage, or impacted by malware.
- Any information considered sensitive or confidential should be encrypted.
- Never download university confidential (sensitive) data to a portable device unless the device is encrypted.
- Licensed software, provided by the university, is solely for university equipment unless otherwise specified. A standard list of permissible software packages is available and maintained by the PC Services group. If additional software packages are needed, they should be reviewed and purchased in accordance with the IT Department to ensure compliance with university policies and security posture.
- Do not store any personal information on university equipment, the university cannot guarantee the confidentiality of information stored on any networked device. The information/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
- Attend security awareness training to improve the cyber security posture of the university.

f. Reporting issues and System Documentation

From time-to-time information resources will have technology issues. It is imperative that these are reported in a timely manner. In addition to reporting a technology device or function not working, users should also report any abnormal behavior with their device(s), accounts or observed weaknesses in cyber security upon noting the behavior.

If a person or department creates a production system, that departmental supervisor is responsible for fully ensuring that creation of documentation, subsequent contingency plan, and ensure the security of all data

therein.

g. Circumventing Security

Users play a pivotal role in cyber security and are entrusted to report any issues, compromises, or vulnerabilities they identify.

- Users may encounter one or all of these threats. In doing so it is the responsibility of the user to notify the Information Technology Security Manager or Director of Information Technology immediately upon doing so.
- Users must not intentionally seek information, browse, obtain copies, or modify files passwords belonging to others unless specifically authorized to do so.
- Users may not seek to add permissions or access to which they do not have a business reason for and therefore are not entitled to.
- Users must refrain from any unauthorized action which deliberately interferes with the operating systems or functions of systems or that is likely to have such effects.
- 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.
- University owned programs and data should not be transferred to other 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 Information technology.
- Users must not attempt to circumvent data protection schemes or uncover security loopholes. This includes creating and/or tuning programs that are designed to identify security loopholes and/or decrypt intentionally secure data. This also includes programs contained within an account, or under the ownership of an account that are designed or associated with security tracking.

V. Definitions

Sensitive data (sensitive information) - is institutional information that must be guarded due to proprietary, ethical, privacy, or business process considerations. Sensitive data must be protected from unauthorized access, modification, transmission, storage or release.

Confidential data (confidential information) - is institutional information protected by government regulations, statues, industry regulations, contractual obligations, or specific university policies. Administrators and data stewards may designate additional type of institutional data as confidential.

Production system - A system that is used to organize or automate office tasks or store information for department/university required purposes. Examples are spreadsheets, single user databases, or even document templates.

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