Acceptable Use of University Information Technology Resources Policy

Policy Statement

To establish and define the "acceptable use" of Marywood University ("Marywood or "University") electronic responses, including, but not limited to, computers, networks, electronic mail services, and electronic information and data, and video services, to support the educational, research and Mission of Marywood University.

This policy is applicable to all faculty, staff, and students, and other individuals using Marywood's network resources, and individuals who are conducting Marywood University business using external networks.

This includes all University owned, licensed, or managed hardware and software, the use of University network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network, and use of information.

I. GENERAL CONSENT

Individuals with access to the University's information technology resources are responsible for their appropriate use, and by their use, agree to comply with all applicable University, policies, guidelines and standards, and applicable state and federal laws and regulations. For use and access to be acceptable, individuals must demonstrate respect of:

- The rights of others privacy;
- Intellectual property rights (e.g. as reflected in licenses and copyrights);
- Ownership of information;
- System mechanisms designed to limit access; and
- An individual's right to be free of intimidation, harassment, and/or retaliation.

II. PRINCIPLES OF ACCEPABLE USE

a) Using only the information technology resources for which they are authorized by the University.
b) Utilizing appropriate authentication mechanisms to access information technology resources.
c) Not attempting to access information technology resources for which their authorization may be erroneous or inadvertent.
d) Only using accounts, passwords, and/or authentication credentials that have been authorized to use consistent with their role at Marywood University.
e) Protecting, and not sharing, their account, password, and/or authentication credentials.
f) Only sharing data with others as defined by applicable policies and procedures, and dependent on their assigned role.
g) Not using Marywood University information technology resources to represent the interest of any non-University group or organization unless authorized by an appropriate University department or office that could be taken to represent Marywood University.

h) Not using any hardware or software designed to assess or weaken security strength, unless authorized by the institutional CISO or his or her designee(s).
i) Not engaging in disruptive "spamming" (i.e., sending unsolicited electronic communication to groups of recipients at the same time), or acting in a way that will harm, damage, corrupt, or impede authorized access to information resources, systems, networks, equipment, and/or data.
j) Not forging identities or sending anonymous messages, unless the recipient has agreed to receive anonymous messages.
k) Not using Marywood University information technology resources to alter, disrupt, or damage information technology resources of another person or entity.
l) Not using Marywood University information technology resources to upload, download or distribute copyrighted or illegal material which results in violation law.
m) Complying with all licenses and contract related to information technology systems which are owned, leased, or subscribed to by Marywood University, and complying with applicable local, state or federal laws, and institutional policies, rules, and guidelines as they relate to information technology resources.

III. PROTECTING THE SECURITY AND INTEGRITY OF INFORMATION RESOURCES FROM UNAUTHORIZED USE:

In order to protect the security and integrity of Information Technology resources against unauthorized or improper use, and to protect authorized individuals from the effects of any potential abuse or negligence, Marywood University reserves the rights, at its sole discretion, to limit, restrict, or terminate any account or use of Information Technology resources, and to inspect, copy, remove or otherwise alter any data, file, or system resources that may undermine authorized use. Marywood University also reserves the right to inspect or check the configuration of Information Technology Resources for compliance with this policy, and to take such other actions as in its sole discretion it deems necessary to protect Marywood Information Technology resources. The University also reserves the right to control and/or manage use of the frequency spectrum within the boundaries of all University locations. Individuals of the University are required to report transmitting devices and their characteristics to University officials, if so requested. The University reserves the right to require those units or individuals found to have such devices that interfere or are suspected to interfere with operation of centrally managed University systems, to discontinue use of such devices, and, if necessary, to remove them from University property.

The University shall not be liable for, and the individual assumes the risk of, inadvertent loss of data or interference with files resulting from the University's efforts to maintain the privacy, integrity and security of the University's Information Technology resources.

The University is not responsible for the content of individuals' personal web spaces, nor the content of servers, programs or files that individuals maintain either in their personally allocated file areas on University-owned computer resources or on personally-owned computers connected to the University's Information Technology Resources.

The University reserves the right to suspend network access or computer account(s), or to impose sanctions as defined in this policy if individually-maintained files, programs or services are believed to have been operating in violation of either law or policy. Additionally, the University retains the right subject to applicable law and policy to search and/or seize, for investigative purposes, any personal hardware or systems connected to University Information Technology resources if there is cause to suspect that such hardware or systems were used either in violation of federal, state or local law, or in violation of the terms and conditions set forth in University policies governing computer and network usage. Restoration will be at the sole discretion of the University. The University shall, to the full extent required under law, cooperate with all legal requests for information, including, but not limited to, disclosure of system user account information when made by any law enforcement officer or legal representatives pursuant to court order, subpoena or other legal process.

The University can enforce the provisions of this policy and the rights reserved to the University without prior notice to the user.

IV. EXCEPTIONS AND EXEMPTIONS:

Exceptions to, or exemptions from, any provision of this policy or supplemental IT guidelines and standards must be reviewed by the Office of Information Technology in accordance with the other IT Policies.

Any questions about the contents of this policy or supplemental IT Guidelines and Standards should be referred directly to the Chief Information Officer (ops@marywood.edu) who has the responsibility to interpret the Security Standards.

POLICY VIOLATIONS:

Any Marywood University department or unit found to operate in violation of this policy may be held accountable for remediation costs associated with a resulting information security incident or other regulatory non-compliance penalties, including but not limited to, financial penalties, legal fees, and other costs.

Faculty, staff, or students who violate this policy and supplemental IT Guidelines and Standards may be subject to appropriate disciplinary action, specifically including suspension r termination of access and/or network privileges.

Procedures

N/A

Related Policies

Asset Management
IT Security Framework
End User Responsibilities
IT Security for IT and Data Professionals
IT Configuration Management
IT Security and Incident Response
IT Security for 3rd Party Partners and Providers

History of the Policy 3/10/2023: The President of the University approved this policy as recommended by the Policy Committee of the University.

MARYWOOD UNIVERSITY
POLICIES AND PROCEDURES MANUAL

Mary Theresa Gardier Paterson
Secretary of the University and General Counsel