Marian University Computer Use-Technology Policy

Revised April 20, 2012

Statement of the Policy

This document constitutes the Marian University policy for the management of computer networks and applies to all uses of IT Resources. Any individual or entity using IT Resources consents and agrees to comply with all of the terms and conditions set forth in this policy, all other applicable University policies and regulations, and applicable local, state and federal laws and regulations concerning the use of IT Resources.

The following use of IT Resources are prohibited:

- Circumvention of any security measure of Marian University or other entity.
- Intentional use, distribution or creation of viruses, worms, or other malicious software.
- Unauthorized copying or unauthorized distribution of licensed software or copyrighted material.
- Accessing data that is not publicly available, does not belong to the user and for which the user does not have explicit permission to access; or accessing IT Resources in a manner designed to circumvent access limitations to public or restricted-access data (e.g., replicating a database by automated queries) without permission.
- Use of IT Resources that disables other IT Resources, consumes disproportionate IT Resources such that other users are denied reasonable access to those resources or materially increases the costs of IT Resources.
- Use of IT Resources for intended to harm others through harassment, libel, slander, fraud or misrepresentation
- Destruction of or damage to equipment, software, or data belonging to the University or others
- Disruption or unauthorized monitoring of electronic communications
- Unauthorized scanning of network nodes
- Unauthorized copying or transmission of copyright-protected material
- Use of the University's trademarks, logos, insignia, or copyrights without prior approval
- Unauthorized use of computer accounts, access codes (including passwords), network, or identification numbers (including email addresses) assigned to others
- Use of computer communications facilities in ways that unnecessarily impede the computing activities of others (such as randomly initiating interactive electronic communications or e-mail exchanges, overuse of interactive network utilities or bandwidth)
- Use of computing facilities for private business purposes unrelated to the mission of the University or to University life
- Academic dishonesty or academic honor code violations
- Violation of software license agreements
- Violation of network usage policies and regulations
- Violation of privacy
- Posting, viewing, printing or sending material that is contrary to the mission or values of the University, including but not limited to obscene, pornographic, sexually explicit, or offensive material

Responsibilities of Users

- Network accounts, passwords, and other types of authorization are assigned to individual users and must not be shared.
- Select strong password(s) and passphrase(s) and change them regularly
- Secure unattended computers (e.g., log off, lock, or otherwise make inaccessible), even if you will only be away from the computer for a moment
- Maintain information in a secure manner to prevent access, viewing, or printing by unauthorized individuals
- Take steps to understand "phishing attacks," computer viruses, and other destructive software, and take steps to protect your accounts from such threats (e.g., never reply to emails asking for account passwords or passphrases, never open unsolicited email attachments, never click unknown links, use virus scanning software, apply system patches in a timely manner, etc.).
- Report unauthorized access to, inadequate protection of, and inappropriate use, disclosure, and/or disposal of information, immediately to your campus police
- Users have the responsibility to abide by existing regulations for the protection of sensitive institutional data.

Privacy and Confidentiality

The University reserves the right to inspect and examine any electronic content on any Marian owned or operated communications system, computing resource, or other electronic device at any time. Permission must be granted by the appropriate University officials.

In addition, sources outside the University may, on occasion, request an inspection and/or examination of any Marian owned or operated communications system, computing resource, and/or files or information contained therein. In such cases, the University will release information only if one or more of the following conditions exist:

- When authorized by the owner(s) of the information
- When required by federal, state or local law
- When required by a valid subpoena or court order

Enforcement

The University considers any violation of Responsible Use to be a significant offense and reserves the right to disconnect systems from the network and suspend violators' use of network resources. Violations of Responsible Use shall subject users to the regular disciplinary processes and procedures of the University for students and may result in loss of their computing privileges, and other measures up to and including expulsion from the University. Illegal acts involving University information technology resources may also subject violators to prosecution by local, state, and/or federal authorities.