Policy 01:010 – Use of Information Resources

1. Purpose

This policy promotes the secure, ethical, and lawful use of the Information Technology Resources owned and operated by or on behalf of the University of Montevallo ("University"). Users of University information systems (including subsystems) as well as other workstations, devices, network infrastructure, and other information technology owned or operated by or on behalf of the University are responsible for their activity. This policy establishes requirements for the acceptable use of such resources.

2. Scope

This policy applies to all University faculty, staff, students, official University affiliates, or any other individual, group, or office that directly, or through any agent acting on their behalf, interact with University Information Technology Resources, regardless of affiliation (hereafter, the "User" or "Users").

3. Policy Statement

Access to the University's Information Technology Resources is a privilege, not a right. These resources are intended to facilitate and support the mission of the University. Access is granted to Information Technology Resources exclusively for their use in meeting the University's mission.

Violations of policy or law may result in temporary or permanent loss of technology-related privileges, University sanctions, disciplinary action including immediate termination of employment, expulsion as a student, and/or other legal action.

3.1. Acceptable Use: When using University Information Technology Resources, all Users must:

- Adhere to all applicable laws, regulations, University policies, contractual agreements, and licensing agreements.
- Protect their User IDs, other authentication and authorization mechanisms and systems from unauthorized use. All individuals are responsible for access to University Information Technology Resources by their User IDs and other authentication and authorization mechanisms.
- Access only information to which they have been given authorized access or that is publicly available.
- Use only legal versions of copyrighted software in compliance with vendor license requirements.

- Be considerate in the use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data, degrading services, or wasting computer time, connection time, disk space, printer paper, or other resources.
- Store data classified as Confidential or Restricted only in University approved secured locations.
- Transmit/transport confidential data, information, and information assets only via University approved secured mechanisms.
- Revise passwords and other authentication and authorization mechanisms suspected of compromise.
- Report identified or suspected security incidents to the University Police Department or to Information Services & Technology (IS&T) Solution Center.

3.2. Unacceptable Use: When using University Information Technology Resources, all Users must not:

- Gain access to or use another person's system, files, or data without permission (note that permission from an individual User may not be sufficient. Some systems may require additional authority).
- Reveal a password or other authentication and authorization means to any other individual, even those claiming to be a support technician over the phone or in person.
- Use computer programs to decode passwords or access-control information.
- Attempt to circumvent or subvert system or network security measures.
- Engage in any activity that is intended to harm systems or any information stored thereon, including creating or propagating malware, disrupting services, damaging files, or making unauthorized modifications to University data.
- Make or use illegal copies of copyrighted software, store such copies on University systems, or transmit them over University networks.
- Use Email, social networking sites or tools, or messaging services in violation of laws or regulations or to harass or intimidate another person, for example, by broadcasting unsolicited messages, by repeatedly sending unwanted mail, or by using someone else's name or User ID.
- Waste shared computing or network resources, for example, by intentionally placing a program in an endless loop, printing excessive amounts of paper, or by sending chain letters or unsolicited mass mailings.
- Use the University's systems or networks for commercial purposes, for example, by selling access to your User ID or by performing work for profit with University resources in a manner not authorized by the University.
- State or imply that they speak on behalf of the University or use University trademarks and logos without authorization to do so.
- Transmit commercial or personal advertisements, solicitations, endorsements, or promotions unrelated to the business of the University.
- Send or receive confidential information via the Internet without making reasonable accommodations for the security of such information.
- Modify, without proper authorization, any of the University's information resources and technology, including the work products of others.

- Store confidential data on portable devices or drives that are unencrypted, cloud-based storage systems, or other portable or external media not provided by the University.

4. Definitions

Information Technology Resources: University-owned facilities, technologies, and information resources used for University processing, transfer, storage, and communications. Included in this definition are computer labs, classroom technologies, computing and electronic devices and services, Email, networks, telephones (including cellular), voice mail, fax transmissions, video, multimedia, and instructional materials. This definition is not all inclusive but rather reflects examples of equipment, supplies, and services. This also includes services that are University-owned, leased, operated, or provided by the University or otherwise connected to University resources, such as cloud-based or hosted software, services, and resources.

5. Policy Approval, Review, and Administration

Responsible Office(s):	Information Services & Technology
Responsible Individual:	Chief Information Officer
Effective Date:	09/1986
Last Revision:	08/2024