Policy 01:011 – Information Technology Security Program

1. Purpose

The University of Montevallo ("University") is responsible for ensuring the integrity of University data and for encouraging and enforcing confidential, legal, and ethical standards of data management and use in compliance with all applicable federal and state laws governing disclosure of information. These include but are not limited to: Gramm-Leach-Bliley Act (GLBA), the Family Educational Rights and Privacy Act (FERPA) of 1974, as amended, and the Fair and Accurate Credit Transactions Act (FACTA) and its implementing regulations, commonly known as the "Red Flags Rule" issued by the Federal Trade Commission. This policy defines the University's actions to meet its responsibilities and requirements associated with securing its Information Technology Resources.

2. Scope

This policy applies to all University faculty, staff, students, official University affiliates, or any other individual, group, or office with access to or using University data and/or University Technology Resources University (hereafter, "User" or "Users").

3. Policy Statement

The Information Technology Security Program (ITSP), through the implementation of best practices and routine training, is intended to promote the confidentiality, integrity, and security of the University's data while increasing User accountability and awareness concerning information theft, misuse, and other risks or cyberthreats.

3.1. Program Oversight: The Chief Information Officer (CIO) or designee has primary institutional responsibility for oversight of (a) information security, (b) networks and systems, and (c) training and educating the University community about security responsibilities. The CIO, in consultation with the Technology Advisory Council (TAC) will administer the ITSP.

The Registrar's Office will provide guidance in complying with privacy requirements established for educational records in accordance with FERPA and other regulations.

3.2. Training: Within 30 days of employment, all University employees will undergo training related to (a) safe computing and information security practices, (b) relevant policies and laws, and (c) methods for recognizing and responding to security concerns. Successful completion of training is required annually thereafter. Unit heads are responsible for ensuring that all employees within their Units complete annual information security training.

3.3. Risk Assessment: A written, annual risk assessment will be conducted and shall include (a) an inventory of protected Unit data; (b) an assessment of potential internal and external risks to data security, confidentiality, and integrity; and (c) a written incident response plan.

3.4. Unit Security Plans: Each Unit is responsible for securing relevant data and Information Technology Resources in accordance with the ITSP and with all University policies and applicable laws. Consequently, each Unit will develop, implement, evaluate, and periodically update *written* information security plans that detail the safeguards and security procedures for all Unit data and information covered by this policy. Each Unit is also responsible for securing protected student and educational information in accordance with FERPA and with applicable University policies.

Unit security plans and safeguarding procedures will address the following.

- Physical security measures
- Authentication, authorization, and accountability for accounts, access passwords, etc.
- Security awareness (policy compliance)
- Incident notification and response
- Maintaining virus protection as supplied by IS&T
- Business continuity planning in association with IS&T disaster recovery plan

3.5. Information Security Violations: Information germane to the mission and operation of the University, regardless of its format, is a proprietary asset of the University; therefore, it is essential that University information and information systems be protected from misuse, unauthorized access, modification, destruction, or unauthorized disclosure, whether accidental or intentional. Data stored or accessed through University systems must be securely maintained.

Examples of violations of University policy include but are not limited to:

- Deliberate and/or unauthorized attempts to access or use the University's computers, computer facilities, networks, systems, programs or data or the unauthorized manipulations, including fraudulent transmissions, of any of the above
- Deliberate and/or unauthorized attempts to modify computer equipment, including terminals or other peripherals, or to deny access to such equipment to other users
- Circumventing or attempting to circumvent normal resource limits, log-on procedures, and security regulations
- Storage of sensitive data in non-secure or unencrypted formats or external devices without adequate safeguards
- Use of University computer resources and data for purposes for which they are not intended; i.e., personal or commercial enterprises not consistent with the University's mission; or allowing such use by other individuals
- Deliberate and/or unauthorized activity which causes University computers, computer facilities, systems, programs or data to be inappropriately accessed, used, or transmitted

- Deliberate and/or unauthorized activity which causes non-UM-owned computers, computer facilities, systems, programs or data to be accessed, used or transmitted in an unauthorized manner
- Disregard, abuse, or violation of copyrights, license provisions and other restrictions including copying or redistributing copyrighted software, data or reports without proper, recorded authorization that applies to computer software, networks, or other outside materials
- Any other action that interferes with the proper functioning of University information systems or impinges on another User's rights.

Any authorized or unauthorized User who abuses information technology resources directly or indirectly, damages or destroys any computer, computer system, computer network, program or data, may be subject to disciplinary action including termination, expulsion, and/or prosecution.

3.6. Vender and Affiliate Responsibilities: Data governed by FERPA requires the vendor or affiliate to sign the University FERPA Amendment unless otherwise covered contractually. Financial data placed with a third party requires the third party provide audited statement of security such as SOC1, SOC2, ISO9001, Sarbanes-Oxley 404 or equivalent. When a non-University service provider will have access to data and information covered by this policy, the service provider must agree to provide and maintain adequate safeguards for the University's covered information, in compliance with the GLB Act. All contracts for such service providers must include such compliance language within the contract provisions. The process of selecting a service provider who will have access to covered data and information will include an evaluation of the service provider's ability to safeguard such data and information.

3.7. Use of External Resources, Computers, and Networks: Users who use networks, facilities, or computers not owned by the University, especially to access, use, or manipulate University data, shall adhere to both this policy and all policies and procedures established by the administrators of non-University networks, facilities, or computers. Whether or not an external use policy exists in the location where non-University resources are being used, University policy shall remain in effect and shall be always adhered to.

3.8. Electronic Data Disposal: All computer systems, electronic devices, and electronic media shall be properly cleaned of sensitive data and software before being transferred outside of the University, either as trade-ins, surplus property, or to be disposed of. IS&T is responsible for sanitizing and properly disposing of computer hard drives and other storage devices that are transferred for disposal. Disposal of electronic media, including floppy disks, CDs, and printed reports is the responsibility of the department that purchases or produces them.

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:	05/1999
Last Revision:	08/2024