UNIVERSITY of MONTEVALLO

Policy 01:011 – Information Technology Security Program

Purpose

The University is committed to providing a campus computing environment consistent with its mission. Equal to this commitment is the University's responsibility to ensure the integrity of University data, and to encourage and enforce confidential, legal and ethical standards of management and use of data in compliance with all applicable federal and state laws governing disclosure of information. These include but are not limited to: Gramm-Leach-Bliley (GLB) Act, the Family Educational Rights and Privacy Act of 1974, as amended, (FERPA), 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.

The Information Security Program (ITSP) is intended to promote the protection of the confidentiality, integrity, availability and accountability of the university's data; and to raise the level of awareness concerning information theft, phishing, social engineering and other cyber-threats through training. It is a framework designed to mitigate risk associated with storing data in unsecure formats or media, and with 3rd party vendors. The program applies to everyone who uses, maintains or manages university business processes involving protected data and information including faculty, staff, students, affiliates and vendors.

Responsible Parties

The Chief Information Officer or designate, in consultation with the Executive Cabinet and Technology Advisory Council (TAC) will administer the Program. The Registrar's Office will provide guidance in complying with privacy requirements established for educational records in accordance with FERPA and other regulations. Information Services and Technology (IS&T) will provide guidance to set electronic guidelines for the safeguarding of covered information that is in electronic format.

Training

All employees will undergo training related to safe computing and information security practices, related policies and laws, and methods for recognizing and responding to security concerns within 30 days of employment, and then annually after that.

Departmental Security Plans

Departmental security plans and safeguarding procedures will be evaluated periodically and adjusted as necessary in light of relevant circumstances and, as necessary, will include changes to the ITSP or to the university's business operations which may result from testing and

monitoring of safeguards. Each relevant University business unit is responsible for securing applicable data and information in accordance with this program and with all university policies and applicable laws. Each relevant University business unit must develop and maintain a written security plan that details the safeguards and security procedures for their own data and information located that is covered by this policy. Each University department or office is also responsible for securing protected student and educational records located in that department or office in accordance with FERPA and with applicable University policies.

Departmental security plans and safeguarding procedures will address the following "red flags":

- 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;

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 systems be protected from misuse, unauthorized access, modification, destruction or disclosure, whether accidental or intentional. Data stored in these systems belong to the University and must be maintained in a secure environment. 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 use of UM facilities or equipment to access non-UM-owned computers or networks;
- 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 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 for, abuse of, 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; and
- Any other action that interferes with the proper functioning of the system or impinges on another user's rights.

A University employee or student 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.

Vendors and Affiliates

Placing university data on external or removable devices, or providing access to data that is protected by FERPA, GLB, Sarbanes-Oxley or other State and Federal Laws requires the approval of the divisional VP, Dean or executive with administrative responsibility for that area, and the CIO or the President. Data governed by FERPA requires the vendor or affiliate sign the university FERPA Amendment unless otherwise covered contractually. Financial data placed with a 3rd party requires the 3rd 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.

Use of External Resources, Computers and Networks

Members of the University community 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 adhered to at all times.

Electronic Data Disposal

All computer systems, electronic devices, and electronic media must be properly cleaned of sensitive data and software before being transferred outside of the University, either as trade-ins, surplus property, or as trash. Information Services & Technology is responsible for sanitizing and/or 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.

Violations of this policy may constitute theft and/or unauthorized use of University property, subjecting violators to possible criminal prosecution, if applicable, dismissal or suspension from employment or enrollment, and/or other civil and legal remedies, which may be available.

Approved 5/99

Last Revised 11/19

Note – with the 11/19 revision, policy 01:014 Information Security Program was repealed as applicable items were incorporated into this policy.