UNIVERSITY of MONTEVALLO

# Policy 01:014 – Information Security Program

The University of Montevallo has adopted this Information Security Program for safeguarding confidential and private financial and related information the University receives in the course of business as required by law, including but not limited to the 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. Covered data and information include personal non-public financial information that the University has obtained in the process of offering a financial product or service (examples include offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, payment plans, and other miscellaneous financial services), or such information provided to the University by another financial institution. Examples of personal non-public information could include address, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers. Covered data and information include both paper and electronic records.

The Information Security Program is intended to promote the protection of the confidentiality, integrity, availability and accountability of covered information. The program applies to everyone who uses, maintains or manages University business processes which involve covered data and information. The program, along with University policies on use of University resources and computer resources security, may apply to specific data, computers, computer systems, or networks provided or operated by University departments.

The Vice President for Business Affairs will administer the Program, including all unit plans and safeguarding procedures developed thereunder. The Records Office will provide guidance in complying with privacy requirements established for educational records in accordance with FERPA and other regulations. The Computer Services Office will provide guidance to set electronic guidelines for the safeguarding of covered information that is in electronic format. Unit 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 Program 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 covered 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 covered data and information located in that unit. 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.

Unit security plans and safeguarding procedures will address the following “red flags”:

- physical security measures;
- authentication, authorization and accountability for accounts, campus network activity, access passwords, etc.;
- security awareness (policy compliance);
- risk assessment;
- incident notification and response;
- virus protection;
- disaster recovery/business resumption plan.

When a non-University service provider will have access to covered data and information, 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.

*Approved 5/09*