Purpose

This compliance plan ("Plan") describes Alabama College of Osteopathic Medicine's safeguards to protect non-public, financial-related personal information ("covered information") in accordance with the requirements of the Gramm-Leach-Bliley Act of 1999 (GLBA). The Safeguards Rule of the GLBA, as defined by the Federal Trade Commission (FTC), requires financial institutions, which the FTC explicitly indicated includes higher education institutions, to have an information security program to protect the confidentiality and integrity of personal information.

These safeguards are provided to:

- Ensure the security and confidentiality of covered information;
- Protect against anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of covered information that could result in substantial harm or inconvenience to any customer.
- Safeguarding personally identifiable information in the possession of the college and preventing its breach.

This Information Security Plan also provides for mechanisms to:

- Designate an employee or employees to coordinate the information security program;
- Identify and assess the internal and external risks that may threaten covered information maintained by ACOM;
- Design and implement safeguards to control the identified risks;
- Oversee service providers, including third party contractors, to ensure appropriate safeguards for covered information are maintained;
- Periodically evaluate and adjust the information security program as circumstances change.

Scope

This policy applies to all college, departments, administrative units, affiliated organizations and third party contractors that create, access, store or manage covered information.

Effective Date

Approved March 2012; revised August 2013.

Authority

This plan responds to the Gramm-Leach-Bliley Act of 1999 that mandates protection of customer information, which for universities is primarily student financial information. See section .060, Definitions, for a definition of information covered by this policy.

Policy

The College will develop, implement and maintain a comprehensive information security program that contains administrative, technical, and physical safeguards to protect covered information.

Definitions

1. Covered Information - information that ACOM has obtained from a customer (e.g., a student) in the process of offering a financial product or service, or such information provided to the College by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.
2. Information Security Program - the administrative, technical, or physical safeguards used to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle covered information.
3. Service Providers - any person or entity that receives, maintains, processes, or otherwise is permitted access to covered information through its direct provision of services to the College.

Roles and Responsibilities

1. Director of Information Systems - ACOM - the DIS is responsible for coordinating and overseeing all elements of ACOM's information security program. The DIS will work with appropriate personnel from other offices as needed (such as the Registrar's Office, Internal Audit, and the Division of Financial Services) to ensure protection of covered information.

Information Security Program Elements

1. Risk Assessment

Under the oversight of the DIS, risk and privacy assessments are performed for all information systems that house or access covered information. These risk and privacy assessments shall address unauthorized access, use, disclosure, disruption, modification and/or destruction of information or the information system itself. Further, the assessments shall identify known potential threats, the likelihood of their occurrence and the magnitude of the impact of those threats should they occur.

Internal and external risks at ACOM include, but are not limited to:

- Unauthorized access of covered information by persons within or outside the College
- Compromised system security as a result of human error, vulnerabilities, infection by malicious software, or unauthorized system access
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems
- Unauthorized access through hardcopy files, usb drives, and external data devices, or reports

- Unauthorized disclosure of covered information through third parties and vendors

Risk and privacy assessments are used to determine the likelihood and magnitude of harm that could come to an information system, the affected individual(s), and ultimately the College itself in the event of a security breach. By determining the amount of risk that exists, the College shall determine how much of the risk should be mitigated and what controls should be used to achieve that mitigation.

Both risk and privacy assessments shall be performed prior to, or if not practical, immediately after acquisition of an information system (in the event that the information system is owned/operated by the College) or prior to initial establishment of service agreements (in the event that the information system is owned/operated by a third party on behalf of the College). Further, the risk and privacy assessments shall be reviewed and, where required, updated after three years or whenever a significant change is made to the information system, whichever comes first.

Risk assessment should include consideration of risks in each of the following operational areas, in accordance with the requirements of the GLBA:

a. Employee training and management
   Prior to being granted access to covered information, new employees in positions that require access to covered information (e.g., position in the Division of Financial Services, Registrar, and Student Financial Assistance) will receive training on the importance of confidentiality of student records, student financial information, and other types of covered information, and the risks of not providing appropriate protection. Furthermore, all employees receive annual training in general information technology security. Training also covers controls and procedures to prevent employees from providing confidential information to an unauthorized individual through social engineering or improper disposal of documents that contain covered information. All training will be reviewed and, where needed, updated at least annually.

   All new employees with access to covered information must pass a criminal background check as a condition of employment.

   Each department responsible for maintaining covered information is instructed to take steps to protect the information from destruction, loss or damage due to environmental hazards, such as fire and water damage or technical failures.

b. Information systems, including network and software design, as well as information processing, storage, transmission, and disposal. See section "Related Laws, Regulations, or Policies" below for the policy framework that manages the risk related to information systems associated with covered information.

c. Incident management, including detecting, preventing and responding to attacks, intrusions, or other systems failures. ACOM's strategy for managing IT security incidents, including assessing risks, is described in the "IT Security Incident Reporting and Response Policy" and associated "IT Security Incident Management Procedures".

2. Designing and Implementing Safeguards

Safeguards are necessary to mitigate and control the risks identified through risk assessment. Furthermore, the effectiveness of safeguards' key controls, systems, and procedures should be regular tested to ensure continued protection of covered information. The policy framework for ACOM's information security program that governs the design, implementation, and maintenance of these safeguards is provided in section Related Laws, Regulations, or Policies" below. Protection of covered information is explicitly encompassed by ACOM's comprehensive information security program that protects all ACOM information and technology assets, commensurate with size and complexity of the institution, the nature and scope of activities, and the sensitivity of information assets.

3. Overseeing Service Providers

   In the process of choosing a service provider that will maintain or regularly access covered information, the selection and retention processes shall ensure the ability of the service provider to implement and maintain appropriate safeguards for covered information. Contracts with service providers may include the following provisions:

   a. An explicit acknowledgment that the contract allows the contract partner access to covered information;
   b. A specific definition or description of the covered information being provided;
   c. A stipulation that the covered information will be held in strict confidence and accessed only for the explicit business purpose of the contract;
   d. An assurance that the contract partner will protect the covered information it receives according to commercially acceptable standards and no less rigorously than it protects its own covered information;
   e. A provision providing for the return or destruction of all covered information received by the contract provider upon completion or termination of the contract;
   f. An agreement that any violation of the contract's confidentiality conditions may constitute a material breach of the contract and entitles ACOM to terminate the contract without penalty; and
   g. A provision ensuring that the contract's confidentiality requirements shall survive any termination of the agreement.
   h. ACOM will insure that specific guidelines to educational institution stipulate that contracts/agreements made with vendors will include the following:
      1) Convey limitation on the data (how can the data be used – not for data mining, etc)
      2) Obtain assurance against re-disclosure (no disclosure to third party without written permission)
      3) Be clear about destruction
      4) Verify existence of sound data security plan
      5) Bind individuals to the agreement

4. Program Evaluation and Adjustment

The DIS will periodically review and adjust the information security program as it relates to the GLBA requirements, with input from the College's Security Incident Response Team (SIRT) and relevant stakeholders. Program evaluation should be based on results of testing and monitoring of security safeguard effectiveness and reflect changes in technology and/or operations, evolving internal and external threats, and any other circumstances that have a material impact on the information security program. The Office of General Counsel and the DIS must review any recommended adjustments.

Related Laws, Regulations, or Policies

1. Operations and Management Security Policy
2. Collection, Use and Protection of Social Security Numbers
3. Identity Theft Prevention per the Federal Trade Commission's Red Flag Rules
4. System Development and Maintenance Security Policy
5. Physical and Environmental Security Policy
6. Access Controls Security Policy
7. IT Security Incident Reporting and Response Policy
8. IT Security Incident Management Procedures
9. Data Classification and Security Policy

Questions/Waivers

The Director of Information Systems (DIS) is responsible for this plan. The DIS or designee must approve any exception to this plan. Questions relating to this plan should be directed to ACOM's Chief Dean.