# Office of Financial Aid Information Security Program

This Information Security Program outlines the safeguards the Office of Financial Aid at Emory has implemented in order to follow the objectives of the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule to protect nonpublic financial records, whether in paper, electronic or other form, about a student or other 3rd party who has a relationship with Emory. These safeguards are put in place to:

- Ensure the security and confidentiality of customer records;
- Protect against any anticipated threats or hazards to the security of such records; and
- Protect against the unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to customers.

## 1. INFORMATION SECURITY PROGRAM SCOPE

This program applies to records containing nonpublic financial information about a student or other third party who has a relationship with Emory, whether in paper, electronic or other form that is handled or maintained by or on behalf of Emory or its service providers. For these purposes, the term nonpublic financial information shall mean any information (1) a student or other third party provides in order to obtain a financial service from Emory; (2) about a student or other third party resulting from any transaction with Emory involving a financial service; or (3) otherwise obtained about a student or other third party in connection with provided a financial service to that person.

## 2. INFORMATION SECURITY PROGRAM OFFICERS

Emory University identified and assigned Information Security Program responsibilities to the Director of the Office of Financial Aid and Emory's Chief Information Security Officer (hereinafter "the Program Officers"). The Program Officers may delegate certain responsibilities associated with the Information Security Program to other members of Emory University.

The Program Officers shall:

- Ensure that the necessary and appropriate Information Security Program related policies are developed and implemented to safeguard the integrity, confidentiality, and availability of customer information within the Office of Financial Aid and its service providers.
- Ensure that the necessary infrastructure of personnel, procedures and systems is in place to monitor, audit, and review compliance with all Information Security Program related policies.
- Ensure that mechanisms are in place for reporting incidents and Information Security Program security violations
- Ensure that the annual security awareness training is delivered to all employees and that the training includes the mechanisms for reporting incidents and security violations.
- Identify and assess the internal and external risks to the security, confidentiality, and integrity of customer records that could result in the unauthorized disclosure, misuse, alteration or destructions of these records.
- Assess the sufficiency of the safeguards in place to protect against identified risks.
- Evaluate and adjust the Information Security Program at least annually.

If the Information Security Program Officers are not able to meet the requirements or a responsibility, or are no longer affiliated with Emory University, the aforementioned responsibilities will be assigned to new Information Security Program Officers.

## 3. IDENTIFICATION OF RISKS

Emory University recognizes exposure to the external and internal risks to the security, confidentiality and integrity of customer records could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such records. Such risks are categorized below but not limited to:

- Unauthorized requests or access to printed, faxed, physically stored or electronic records
- Interception of data during transmission
- Loss of data or data integrity

- System failure

Emory's Enterprise Security Team conducts periodic risk and security assessments at the Enterprise and Department levels to assess the sufficiency of the safeguards in place to control the identified risks. Security Assessments are conducted on all new applications to be used and require the appropriate safeguards to be put in place prior to using such applications.

Enterprise level risk assessments for the Office of Financial Aid are based on the NIST Special Publication 800-171 and cover all control domains for the information systems, including access controls, employee awareness and training, configuration management, identification and authentication, incident response, maintenance, media protection, personnel security, physical protection, system and communication protection, system and information integrity and the network and software design where student records are processed and stored.

The Enterprise Security Team, Internal Audit, Office of Compliance and/or third party auditing firms shall conduct periodic additional or targeted risk assessments. All identified risks are tracked until full resolution by the Office of Financial Aid.

Enterprise Security Team is responsible for detecting, preventing and responding to attacks, intrusions and other system failures, while IT Support applies appropriate safeguards to the user workstations, printers/faxes and software. Office of Financial Aid is responsible for reporting the security incidents, and for the periodic evaluations and correction for all identified risks, and security and business process issues, which have direct impact to the security of customer records.

## 4. EMPLOYEE TRAINING AND MANAGEMENT

All new employees in the Office of Financial Aid go through the background check and receive security awareness training prior to obtaining access to work with student records. Enterprise Security Team sends out periodic security reminders to all employees and students to keep them apprised of potential security threats and educate them on emerging concerns. In addition to training new employees, the Office of Financial Aid will also conduct regular training of its personnel on information security at least once a year.

## 5. OVERSIGHT OF SERVICE PROVIDERS

The Information Security Program Officers select and retain only those service providers that are capable of maintaining appropriate safeguards for nonpublic financial information of students and other third parties to which they have access.

The Information Security Program Officers work with the Contract Administration Office, Procurement Services, and the Office of General Counsel to develop and incorporate standard, contractual protections applicable to third party service providers, which require such providers to implement and maintain appropriate safeguards. Any deviation from these standard provisions requires the approval of the Office of General Counsel or other designated institutional official. Software licenses and contracts for the purchase of IT resources that exceed $100,000 must be negotiated through the office of the Enterprise CIO

## 6. ADJUSTMENTS TO THE INFORMATION SECURITY PROGRAM

The Information Security Program Officers are responsible for evaluating and adjusting this Security Program at least annually based on the results of risk assessments, emerging threats, changes to the information systems or software where customer records are stored or processed, changes to the business processes or any other changes that may have a material impact to the Information Security Program.

## 7. RELATED POLICIES

Emory University had implemented comprehensive Information Security policies, which are incorporated by reference into this Information Security Program. These polices are:

- Office of Financial Aid Information Security Policy
- Critical Financial Reporting Systems Security Policy
- Automatic Forwarding of Email from the EmoryExchange or the Emory Office 365 Environment Policy

- Connecting to the Emory Data Network Policy
- Disk Encryption Policy
- Domain Names Policy
- Emory Network IDs (NetIDs) and Passwords Policy
- Enterprise Information Security Incident Response Policy
- Enterprise Password Policy
- Information Technology Conditions of Use Policy
- Internal Mobile App Distribution Policy
- Peer-to-Peer File Sharing Policy
- Records Management Policy
- ResNet Policy
- Smart Device Security Policy
- Confidentiality and Release of Information About Students Policy
- Protecting Student Privacy in Distance Education Policy