Office of Financial Aid Information Security Program

This Office of Financial Aid Information Security Program (the "Information Security Program") outlines the safeguards the Office of Financial Aid at Emory has implemented in order to follow the requirements of the Gramm-Leach-Bliley Act ("GLBA") Safeguards Rule codified at 34 CFR 314.4, to protect the security, confidentiality, availability and integrity of nonpublic personally identifiable financial records, whether in paper, electronic or other form, about a student or other 3rd party who has a relationship with Emory University ("Emory").

The objectives of the GLBA standards for safeguarding information are intended 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

The Information Security Program applies to records containing non-public 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. PROGRAM'S QUALIFIED INDIVIDUAL DESIGNATION AND RESPONSIBILITIES

Emory University designates responsibilities for overseeing and implementing the Information Security Program to its Chief Information Security Officer (the "Program Officer "). The Program Officer may delegate certain responsibilities associated with the Information Security Program to other members of the Emory staff.

The Program Officer shall:

- Ensure that the necessary and appropriate 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 periodic 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 Program Officer is not able to meet the requirements or a responsibility, or are no longer affiliated with Emory University, the aforementioned responsibilities will be assigned to a new Qualified Individual.

3. RISK ASSESSMENT AND SAFEGUARDS

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 confidentiality or data integrity
- System failure

Emory University's Information Security Program provides guidelines to continuously monitors and test systems and application on regularly basis which test the effectiveness of Emory's GLBA safeguards. Those safeguards include but are not limited to the implementation of vulnerability management protocols which continuously run security scans on Emory's system and applications quarterly and monthly as need to safeguard Emory from possible security threats that can be exploited from non-remediated security vulnerabilities. Emory University's Enterprise Security Team conducts internal and external penetration testing on systems that store and transmit PCI and PII information. These controls are put in place to meet the safeguards against the GLBA requirements.

Emory’s Enterprise Security Team conducts periodic risk and security reviews and assessments at the Enterprise and Department levels to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, of customer information and assess the sufficiency of the safeguards in place to control the identified risks. Also, Security (Reviews) 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. Security assessments are conducted on Emory University's research contracts on a case-by-case basis because those contracts may require GLBA safeguards to be put in place to protect (PII) Personal Identifiable Information and sensitive information. Emory Information Systems are monitored for intrusions 24/7 via a SOC (Security Operation Center) team. OIT Enterprise Security reviews the resulting alerts on a daily basis (Monday through Friday) or as escalated by the SOC.

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. Additionally, all Emory faculty and staff are required to take security awareness training.

5. OVERSIGHT OF SERVICE PROVIDERS

The Program Officer shall 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 Department OIT (GRC) continuously conducts a Third-Party Vendor assessment as well as Third-Party applications assessments.

The Program Officer shall 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 Program Officer 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. INCIDENT RESPONSE PLAN

Emory University’s Enterprise Information Security Incident Response Policy sets forth an incident response plan that is designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information.

8. GLBA REPORTING

The Program Officer shall submit an annual written report, with appropriate partners, to the appropriate governing body on the overall status of the Information Security Program and Emory's compliance with GLBA.

9. RELATED POLICIES

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

- Office of Financial Aid Information Security Policy
- Critical Financial Reporting Systems Security Policy
- Automatic Forwarding of Email from the Emory Exchange 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