Lu Ross Academy

GLBA Information Security Program

This Information Security Plan describes safeguards implemented by Lu Ross Academy to protect covered data and information in compliance with the FTC's Safeguards Rule promulgated under the Gramm Leach Bliley Act (GLBA). These safeguards are provided to:

Ensure the security and confidentiality of covered data and 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 data and information that could result in substantial harm or inconvenience to any customer.

This Information Security Program also identifies mechanisms to:

Identify and assess the risks that may threaten covered data and information maintained by Lu Ross Academy;

Develop written policies and procedures to manage and control these risks;

Implement and review the program; and

Adjust the program to reflect changes in technology, the sensitivity of covered data and information and internal or external threats to information security.

Purpose:

The Federal Trade Commission's Safeguards Rule, which implements the security provisions of the Gramm-Leach-Bliley Act (GLBA)/Program, went into effect on May 23, 2003. The Safeguards Rule requires financial institutions, which includes colleges and universities that are significantly engaged in providing Financial Services, to protect the security, confidentiality, and integrity of customer financial records, including non-public personally identifiable financial information. To ensure this protection, the GLBA Safeguards Rule mandates that all covered financial institutions establish appropriate administrative, technical and physical safeguards (Reference 16 CFR § 314.1(a)).

All data, personnel, devices, systems, and facilities that enables the school to achieve business purposes in accordance with their relative importance to business objectives that involve customer personal financial records fall within the purview of this policy. This includes paper records, electronic records that are necessary to achieve student success and the acquisition of Title IV funds.

Policy Statement:

GLBA mandates that the Academy appoint an Information Security Program Coordinator, conduct a risk assessment of likely security and privacy risks, Academy a training program for all employees who have access to covered data and information, oversee service providers and contracts, and evaluate and adjust the Information Security Program periodically.

Information Security Program Coordinator(s)

The School President and the information technology consultant have been appointed as the coordinators of this Program at Lu Ross Academy. They are responsible for assessing the risks associated with unauthorized transfers of covered data and information, and implementing procedures to minimize those risks to the Academy. Internal Audit personnel will also conduct reviews of areas that have access to covered data and information to assess the internal control structure put in place by the administration and to verify that all departments comply with the requirements of the security polices and practices delineated in this program.

Identification and Assessment of Risks to Customer Information

Lu Ross Academy recognizes that it is exposed to both internal and external risks, including but not limited to:

- Unauthorized access of covered data and information by someone other than the owner of the covered data and information
- Compromised system security as a result of system access by an unauthorized person
- 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 of covered data and information by employees
- Unauthorized requests for covered data and information
- Unauthorized access through hardcopy files or reports
- Unauthorized transfer of covered data and information through third parties
- Unauthorized disposal of Covered Data; and
- Unsecured disposal of Covered Data.

Student/customer physical data is kept in a locked office inside locked fireproof file cabinets. Two years after student graduation, files are transferred to a secure file storage facility. Ten years after graduation, files are destroyed by the storage facility.

LRA recognizes that this may not represent a complete list of the risks associated with the protection of covered data and information, and that new risks are created regularly, Lu Ross Academy Cyber Security will actively participate and monitor appropriate cybersecurity advisory groups for identification of risks. Since technology changes over time, the possibility of new risks may arise. LRA's data owners and custodians will actively seek to identify and address all potential technology security risks associated with Covered Data.

Current safeguards implemented, monitored and maintained by Lu Ross Academy Cyber Security are reasonable, and in light of current risk assessments are sufficient to provide security and confidentiality to covered data and information maintained by the Academy. Additionally, these safeguards reasonably protect against currently anticipated threats or hazards to the integrity of such information.

Employee Management and Training

References and/or background checks (as appropriate, depending on position) of new employees working in areas that regularly work with covered data and information (e.g. Finance Division, Financial Aid) are checked/performed. During employee orientation, each new employee in these departments receives proper training on the importance of confidentiality of student records, student financial information, and all other covered data and information. Each new employee is also trained in the proper use of computer information and passwords. Training includes controls and procedures to prevent employees from providing confidential information to an unauthorized individual, as well as how to properly dispose of documents that contain covered data and information. These training efforts should help minimize risk and safeguard covered data and information.

Physical Security

Lu Ross Academy has addressed the physical security of covered data and information by limiting access to only those employees who have a legitimate business reason to handle such information. For example, financial aid applications, income and credit histories, accounts, balances and transactional information are available only to Lu Ross Academy employees with an appropriate business need for such information. Furthermore, each department responsible for maintaining covered data and 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.

Safeguarding Paper Information

Secure Covered Data by locking fire safe file cabinets and offices when not in use.
Do not leave Covered Data unattended and unsecured.
Access to Covered Data shall only be granted to those who need such access.
Comply with other applicable Academy policies and procedures including, but not limited to, Lu Ross Academy's records retention schedule.

Safeguarding Electronic Information

Lu Ross academy uses password-protected computers and systems with access to Covered Data.
Computers and systems are "logged off" when access to Covered Data is no longer needed.
LRA shuts down and turns off computers at the end of each day where possible.
Covered Data are not left unattended and unsecured.
Access to computers and systems shall only be granted to those who need such access.
A multi-factor authentication system is used to access customer data. Users who need access must first log on to a password protected computer. Then, access to the RGM System which contains customer/student data requires an additional password. Passwords are changed every three months.
Covered Data is then encrypted when transmitting or storing it electronically. Lu Ross Academy uses a Third Party Servicer, RGM Systems, which encrypts all stored data on their system. The Academy does not download any data from the RGM system to local hard drives.
Monitor systems for actual or attempted attacks, intrusions, or other systems failures.

Information Systems

Access to covered data and information via Lu Ross Academy's computer information system is limited to those employees and faculty who have a legitimate business reason to access such information. The Academy has policies and procedures in place to complement the physical and technical (IT) safeguards in order to provide security for Lu Ross Academy's information systems. These policies and procedures, listed in Section 3 below, are available upon request from the Director of Information Technology.

Social security numbers are considered protected information under both GLBA and the Family Educational Rights and Privacy Act (FERPA). As such, Lu Ross Academy has discontinued the use of social security numbers as student identifiers in favor of the student ID# as a matter of policy. By necessity, student social security numbers will remain in the student information system; however, access to social security numbers is granted only in cases where there is an approved, documented business need.

Management of System Failures

Lu Ross Academy IT Department has developed written plans and procedures to detect any actual or attempted attacks on Lu Ross Academy systems and has an Incident Response Plan which outlines procedures for responding to an actual or attempted unauthorized access to covered data and information. This document is available upon request from the Director of Information Technology

Oversight of Service Providers

GLBA requires the Academy to take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. This Information Security Program will ensure that such steps are taken by contractually requiring service providers to implement and maintain such safeguards. The Security Program Coordinator(s) will identify service providers who have or will have access to covered data and will work with Lu Ross Academy's outside Legal Counsel and other offices as appropriate, to ensure that service provider contracts contain appropriate terms to protect the security of covered data. Lu Ross Academy's Third Part Servicer, RGM has their own Cyber Security policy and safeguards.

Continuing Evaluation and Adjustment

This Information Security Program will be subject to periodic review and adjustment, at least annually. Continued administration of the development, implementation and maintenance of the program will be the responsibility of the designated Information Security Program Coordinator(s), who will assign specific responsibility for technical (IT), logical, physical, and administrative safeguards implementation and administration as appropriate. The Information Security Program Coordinator(s), in consultation with Lu Ross Academy's outside legal counsel, will review the standards set forth in this program and recommend updates and revisions as necessary; it may be necessary to adjust the program to reflect changes in technology, the sensitivity of student/customer data, and/or internal or external threats to information security.

Policy Terms:

Covered data and information

Covered data and information for the purpose of this program includes student financial information (defined below) that is protected under the GLBA. In addition to this coverage, which is required under federal law, Lu Ross Academy chooses as a matter of policy to include in this definition any and all sensitive data, including credit card information and checking/banking account information received in the course of business by the Academy, whether or not such information is covered by GLBA. Covered data and information includes both paper and electronic records.

Pretext calling

Pretext calling occurs when an individual attempts to improperly obtain personal information of Lu Ross Academy customers to be able to commit identity theft. It is accomplished by contacting the Academy, posing as a customer or someone authorized to have the customer's information, and through the use of trickery and deceit (sometimes referred to as, social engineering), convincing an employee of the Academy to release customer-identifying information.

Student financial information

Student financial information is that information that Lu Ross Academy has obtained from a student or customer in the process of offering a financial product or service, or such information provided to the Academy 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.