Loyola Marymount University Non-Public Personal Information Policy
Gramm-Leach-Bliley Act (GLBA)
Effective May 23, 2003

On November 12, 1999, the Gramm-Leach-Bliley Act (GLBA) was passed into law. The Federal Trade Commission requires Financial Institutions to ensure the security and confidentiality of Non-Public Personal Information (NPI) as of May 23, 2003. For purposes of administering the act, Colleges and Universities must ensure that NPI is secure, confidential, and protected from unauthorized access and threats. The following safeguarding policies and practices are administered at Loyola Marymount University. (LMU)

1. The University has established the Office of the Registrar as the administrative office responsible for ensuring that compliance to GLBA is followed by Students, Faculty, Administrative, and affiliated entities with the University.

2. Loyola Marymount University only discloses information only as necessary to perform specific functions and responsibilities required to meet it's Academic and Business Mission. NPI will not be provided to individuals or organizations where such information is not required to achieve its contracted objective.

3. Loyola Marymount University contracts with service providers who are capable of maintaining and safeguarding customer information as required by GLBA.

4. Loyola Marymount University utilizes appropriate safeguards to protect Personal and Non-Personal Public Information, (NPI) such as but not limited to, network firewall, data encryption, user, password, and pin number protection, data back-up and redundancy to prevent the unauthorized use/theft, or compromising of customer non-public personal information.

5. Faculty, Administrators, and Staff employees with access to NPI are trained in policies and procedures to maintain strict confidentiality of customer non-public personal information. Questions regarding appropriate disclosure of NPI will be directed to the Compliance Officer.

6. The University publishes a clear and conspicuous NPI safeguard policy electronically and is available for public review.

7. The University administers an information risk assessment program to evaluate the current effectiveness of NPI safeguarding controls and procedures. Examples of areas that have significant non-public personal information are Human Resources, Information Technology Services, Admissions, Registrar, Business Finance and Controllers, Financial Aid, Student Health, Residence Life, University Extension, Business Affairs and Mail Distribution Center, and the Offices of Student Affairs and University Relations.

The Federal Trade Commission's regulations implementing the GLBA specifically provides that colleges and universities will be deemed to be in compliance with privacy provisions of the GLBA if they are in compliance with the Federal Family Education Rights to Privacy Act (FERPA), however, the University strives to maintain customer financial and non-personal information security programs, assess the needs for employee information security training, and include contractual requirements in agreements with third parties that have access to financial and non-personal information covered by GLBA. Other details of LMU's comprehensive safeguarding plan are contained within the attached appendix.

GLBA Appendix. Securing Information

Employee Management and Training Procedures

Shall include:

Check references prior to hiring employees who will have access to customer information.
Require employees to sign an agreement to follow LMU's confidentiality and security standards for handling customer information.
Employees are trained to take basic steps to maintain security, confidentiality, and integrity of customer information, such as

- locking rooms and cabinets containing paper records
- properly shred and recycle documents sensitive information
- using password activated screen savers
- using strong passwords (min 8 characters)
- routinely require password prompted changes
- encryption of sensitive customer information when it is transmitted electronically over networks or stored online
- referring calls or other request for customer information to designated individuals who have had safeguards training, and recognizing fraudulent attempts to obtain customer information and reporting to appropriate law enforcement agencies.
- limits access to customer information to employees who have a business reason for seeing it.
- Consumers are cautioned against transmission of sensitive data via email. Advise customers to utilize password protection in transmitting sensitive information.

Information Systems

Security is maintained throughout the life cycle of customer information as follows- that is from data entry to data disposal.

- Electronic information is stored in secure locked computer centers, protected against destruction and damage form potential physical hazards.
- Electronic Customer information is maintained on as physically secure dedicated server accessible by password.
- Sensitive information is not stored on a machine with a non secure internet connection.
- data is secured on back-up media and archived for both on-site and off-site disaster recovery.
- E-Commerce and other Credit Card data is collected utilizing servers that employ top level SSL encryption software.
- Customer information is disposed of in a secure manner, outdated information residing on hardware no longer in use is completely erased, and such hardware is effectively destroyed.

Managing System Failures

The following procedures are endorsed to prevent, detect, and respond to attacks, intrusions or other system failures.

- ITS maintains a written contingency plan to address any breaches of physical, administrative or technical safeguards
- Routinely applies vendors software patches that resolve vulnerabilities, and maintain automatic anti-virus software updates.
- ITS maintains up-to-date firewalls and provides central management of security tools for ITS employees.
- Routinely back-up all non-personal customer information regularly.
- Notifies customers promptly if their Non-public personal information is subject to loss damage or unauthorized access.