DIVISION: **Administration**	
SUBJECT: Information Security Policy	Page 1 of 11
Policy Number:	Supersedes: **None**
Effective Date: 9/10/2009	Previous Issued: **N/A**

1.0 STATEMENT OF POLICY

The Loyola Marymount University Information Security Policy defines the role of information security in supporting the mission of the University, while fostering an environment to protect the University community from information security threats that may compromise the confidentiality, availability, privacy, and integrity of all information assets. The policy applies to anyone using Loyola Marymount University information technology resources, including, but not limited to, students, faculty, staff, visitors, and guests.

2.0 DEFINITION

2.1 **Confidential Information –** Data classified by the University not to be divulged to the public realm. This may include non-public personal information (NPI), personally-identifiable information (PII), protected health information (PHI), or other information sensitive to the business of the University.

2.2 **Confidentiality, Integrity, and Availability Paradigm** – Also known as the CIA triad, confidentiality, integrity, and availability form the core principles of information security. The concept of confidentiality includes the prevention of unauthorized use or access to data. The concept of integrity is the prevention of data being created, changed, or deleted without authorization. The concept of availability is that data and the resources used to process data are available and functioning properly.

2.3 **Data Access Authorizers -** Unit heads or individuals delegated authority in accordance with established procedures by unit heads or higher level management in their organizational reporting chain to authorize and initiate access requests to data.

2.4 **Data Custodian** - Information Technology Services is the data custodian. The custodian is responsible for providing a secure infrastructure in support of the data, including, but not limited to, providing physical security, backup and recovery processes, granting access privileges to system users as authorized by data trustees or their designees (usually the

data stewards), and implementing and administering controls over the information.

2.5 **Data Steward** - Data stewards are University officials having direct operational-level responsibility for information management – usually department heads. Data Stewards are responsible for data access and policy implementation issues regarding data that originates from University processes maintained by the Data Steward

2.6 **Data User** - Data users are individuals who need and use University data as part of their assigned duties or in fulfillment of assigned roles or functions within the University community. Individuals who are given access to sensitive data have a position of special trust and as such are responsible for protecting the security and integrity of those data.

2.7 **Data Views** - A logical collection of data elements, possibly from multiple physical databases, that are assembled and presented according to a defined set of rules.

2.8 **Information Assets** - Data maintained by the University to support the business of the University and its mission. Data may include information stored in University-maintained information systems or hosted by a third-party.

2.9 **Information Security** - The process of protecting data from unauthorized access, use, disclosure, destruction, modification, or disruption.

2.10 **University Data -** A data element is considered University Data if it satisfies one or more of the following criteria:

- It is relevant to planning, operating, managing, or auditing a major administrative function at Loyola Marymount University; or
- It is referenced or required for use by more than one organizational unit; or
- It is included in an official Loyola Marymount University administrative report; or
- It is used to derive an element that meets the criteria above.

2.11 University Process - A systematic series of actions performed by a unit of the University with an intended end.

3.0 INFORMATION SECURITY IDEALS

3.1 Support University Mission

This Information Security Policy is created with the University's mission in mind in an effort to balance the University's ability to conduct operations while maintaining an acceptable level of risk in protecting the University's information resources.

3.2 Comply with Federal and State Laws

Loyola Marymount University will abide by all local, state, and federal laws pertaining to information security and privacy in the pursuit of protecting non-public personal information (NPI) and personal health information (PHI).

3.3 Shared Responsibility and Accountability

All members of the University community share in the responsibility for protecting the University's information assets and resources for which they have access or custodianship.

3.4 Security Awareness

All members of the University share in the belief that education is a major tenet in protecting the University, its assets and users from cyber threats.

4.0 ROLES AND RESPONSIBILITIES

4.1 All Members of the Campus Community

All campus members including contractors and guests are expected to comply with all federal, state, and local laws pertaining to the protection of confidential information as well as campus policies meant to protect the security of information systems on campus. In general, the responsibility of each and every campus user includes being aware of and practicing safe computing habits. A list of safe computing standards are outlined in Appendix A.

4.2 Managers and Supervisors

The responsibilities of administrative officials include those of all members of the campus community outlined in Appendix A in addition to ensuring that their subordinates are appropriately provisioned to the information resources required to perform the duties of their job. This includes ensuring that accounts are modified or terminated when subordinates are transferred to other job duties or terminate relations with the University.

4.3 Information Technology Department

All Information Technology personnel are expected to comply with all responsibilities of campus users in addition to the responsibilities in Appendix B.

4.4 Director of Information Security and Compliance

The role of the Director of Information Security and Compliance is to identify, develop, and implement information security actions in support of the University mission and information security policy. He/She will also keep abreast of all current and pending legislation related to information security and privacy at the local, state, and federal levels. He/She is responsible for providing a secure infrastructure in support of the data, including, but not limited to, providing physical security, backup and recovery processes, granting access privileges to system users as authorized by data custodians or their designees (usually the data stewards), and implementing and administering controls over the University data. The Director of Information Security and Compliance will also be responsible for providing information security awareness training to the campus community.

4.5 Chief Information Officer

The role of the CIO is to lead the University's activities regarding information technology. The CIO will lead IT staff in carrying out the University's Information Security Policy and ensuring the security of all University information systems and protection of the confidentiality, availability, privacy, and integrity of all data on such systems.

5.0 DATA CLASSIFICATION

Information resources and the data contained within these resources are considered to be assets of the University. Data classifications are based on risks associated with the processing and storage of this information graded into three levels of protection – Restricted, Sensitive, and Public.

5.1 Data Classifications

5.1.1 Restricted

Data available only to designated personnel who require access to perform their job functions. Restricted data includes any data element that is protected by state and/or federal privacy legislation such as social security numbers, driver's license numbers, student data not identified as directory information, employee records, personal financial information, and personal health information. Data classified as Restricted generally has mandates for disclosure when unauthorized persons gain access to this information.

5.1.2 Sensitive

Any data element that is not protected by federal or state legislation and is not appropriate for public consumption. Data classified as Sensitive may include organizational finance, donor information, audit documents, building schematics or any other data element or collection of data or information that should be available to those on a needs to know only basis.

5.1.3 Public

Data elements generally available for public consumption. Examples of this type of data include directory information such as department names, building names, and other non-personally-identifiable information (non-PII) as well as any information provided for the purpose of informing the public or required by law.

6.0 DATA ACCESS SECURITY

The Data Access Policy serves to provide direction in granting access to University data in accordance with the Data Classification policy. Access to data will be granted by data stewards who require access in the performance of official University business without violating legal or legislative restrictions.

6.1 Access Responsibilities

6.1.1 Inquiry-type access to official University Data will be authorized to individuals who require access in the performance of official University business without violating legal, federal, or state restrictions.

6.1.2 Every Data User granted create and/or write privileges is responsible for their actions while using these privileges. That is, all campus units are responsible for the official University Data they originate, update, and/or delete.

6.1.3 Data Users are expected to respect the confidentiality and privacy of individuals whose records they access, to observe any restrictions that apply to data to which they have access, and to abide by applicable laws or policies with respect to access, use, or disclosure of information. Expressly forbidden is the disclosure or distribution of University Data in any medium, except as required by an employee's job responsibilities. Also forbidden is the access or use of any University Data for one's own personal gain or profit, for the personal gain or profit of others, or to satisfy one's personal curiosity or that of others.

6.2 Coordination of Access

Data Stewards will designate individuals to be Data Access Authorizers to coordinate University Data access for core institutional data such as Financial, Human Resources and Student data. The Data Custodian will receive requests from Data Access Authorizers and maintain records of authorized Data Users. Employees may request access to data through a designated Data Access Authorizer.

6.3 Request for Review

Data Users may request that the Data Steward and Data Access Authorizer review the restrictions placed on a data element or Data View. All such requests will be submitted through an Data Access Authorizer.

6.4 Dispute Resolution for Data Access

In the event of a dispute regarding specific access to data arises, an objective ad-hoc committee chaired by the VP for Information Technology Services will entertain final appeals to resolve disputes and make a recommendation to the Provost. Members of this ad-hoc committee will be comprised of those other than Data Stewards and Data Access Authorizers. All appeal decisions made by the Provost are final.

7.0 DATA RETENTION

The Data Retention policy states that all data regardless of paper or digital format will be retained for a minimum period as required by law, or usefulness to the University prior to its lawful destruction. The University Records Retention and Disposal policy is maintained by the Office of Risk Management.

8.0 PHYSICAL SECURITY

8.1 Infrastructure Assets

The physical security of electronic devices and cable plant that reside in or transmit University data should be protected from unauthorized physical and remote access. Infrastructure assets include servers, network devices such as routers, switches, firewalls, monitoring equipment, wireless access points. Cable plant includes, but not limited to copper and fiber termination points.

8.2 Infrastructure Storage

Information assets should be stored in locked rooms with limited access to authorized personnel only. These rooms should not be used for storage of any kind including janitorial supplies, department surplus or office supplies. Whenever possible, infrastructure assets should be placed in rooms designated for information technology use only.

8.3 Infrastructure Access

8.3.1 Access to infrastructure assets should be limited to information technology staff as designated by the Chief Information Officer or Director of Information Security, Public Safety supervisors, University locksmiths, electricians, HVAC personnel and approved contractors.

8.3.2 All non-LMU employees must notify Information Technology Services prior to entering a room containing infrastructure assets maintained by Information Technology Services.

9.0 ENFORCEMENT

Violations of this and related policies will be handled according to existing University disciplinary procedures. Violations of local, state, federal, or other laws will be reported to the appropriate authorities as required by law.

10.0 REVIEW

This policy will be reviewed and updated as needed, at least annually, based on the recommendations of the Director of Information Security and Compliance. The responsibility of reviewing and proposing changes to this policy lies with the Director of Information Security and Compliance.

Last reviewed by: David Meske All IT Directors	Date: July 20, 2009 April 8, 2009
Approved by:	Date:
Denied/Postpone:	Date:
Notes:	

Appendix A: Safe Computing Standards

Computer

- Maintain computer operating system with latest security patches.
- Maintain computer applications by installing updates when prompted.
- Maintain anti-virus software with latest virus definitions.
- Don't install recreational programs and games on LMU-owned computers.

Passwords

- Use secure passwords to access any computer used to access the campus network.
- Keep computer monitor and desktop area clear of any hand written passwords.
- Do not share passwords with anyone.

Data Protection

- Secure computer from unauthorized access when unattended.
- Shred all discarded hard copies of confidential information.
- Securely destroy all unneeded instances of files, whether digital or paper that contain non-public personal information (e.g. SSN, driver's license number, transcripts, grades, etc).
- Do not copy non-public personal information (NPI) or personal health information (PHI) to mobile media without written permission from the respective data steward.

Email

- Never respond to email requests asking for your passwords or other account information.
- Only open attachments when you are sure it is safe to do so.
- Only click on embedded links to websites when you are sure it is safe to do so.

Help

- Report suspected computer security incidents to the Technology Helpdesk immediately at (310) 338-7777 or helpdesk@lmu.edu.

Appendix B: Information Technology Services Responsibilities

- User passwords cannot be reset without confirming user identity.
- Users should not be requested to divulge their passwords at any time.
- All vendor, auditor, or consultant access to any information system must be approved by supervisory personnel prior to access.
- Access to, or possession of, any information system or data stored on such systems enforced by a court-ordered search warrant must be approved in writing by the University President or their designee.
- Access to or possession of any information system or data stored on such systems by law enforcement will not be granted without a search warrant.
- Practice safe computing standards at all times.
- Do not abuse administrative access.

Appendix C: Current List of Data Stewards and Data Access Authorizers

The following list of Data Stewards is not meant to be a comprehensive list, but rather a guide for identifying stewards for the more common data elements. Organizational units that create subsets of student, employee, alumni or other data should identify a data steward for the data that the organizational unit creates and maintains

Data Stewards

Student Data	VP for Enrollment Management
Employee Data	V.P. Human Resources
Alumni Data	Associate VP for University Relations

Authorized Requestors

Student Data

Matt Fissinger, Director of Admissions
Jorge Atilano, Sr. Admissions Analyst
Louisa Vakili, Director of Financial Services,Bursar
Jennifer Stech, Asst. Bursar
Catherine Graham, Director of Financial Aid
Vic Soldo, Assoc. Director of Enrollment
Kathy Reed, Associate Registrar
Robert Nitsos, Assistant Registrar

Employee Data

Tracy Martin, Director for Human Resources/HRIS & Compensation

Financial Aid Data

Catherine Graham, Director of Financial Aid
Vic Soldo, Assoc. Director of Enrollment

Alumni Data

Alma Vorst, Senior Director of University Relations Services