Loyola University

Office of Information Technology

Information Security Policy

Purpose

The purpose of this policy is to ensure the confidentiality and integrity of Loyola's information assets. The policy reflects Loyola's commitment to the protection of sensitive personal and critical business information. Loyola and its staff acknowledge the presence of many threats to information security and the importance of protecting the privacy of the University community, safeguarding vital business information, and fulfilling legal obligations.

(This policy serves as a companion to the Loyola Network Security Policy, which speaks to the secure configuration of systems and use of the Loyola network.)

Scope

This policy applies to the entire Loyola community, including students, faculty, staff, alumni, trustees, temporary employees, contractors, volunteers and guests who have access to Loyola information assets.

Information assets are defined as information in any form, recorded on any media. Such assets include data, images, text, software, and voice recordings, in digital or analog form, stored on hardware, paper or other storage media.

Information Classifications

a. **Public**

This classification covers information assets that have already been disclosed or made available to the general public by an official of the University. Although security mechanisms are not needed to control disclosure and dissemination, they are still required to protect against unauthorized modification and/or destruction of information.

b. **Internal**

This classification covers information assets that require protection against unauthorized disclosure, modification, destruction, and use, but the sensitivity of the information is less than that for confidential information. Examples of Internal-use-only information are internal memos, emails, correspondence, and other documents whose distribution is limited as intended by the provider or sender. The University's Intranet is included in this topic.

c. **Confidential**

This classification covers sensitive information assets about individuals and sensitive information assets about the University. Information assets receiving this classification require

a high level of protection against unauthorized disclosure, modification, destruction, and use. Specific categories of confidential information include personally identifiable information about:

i. Current and former students (whose education records are protected under the Family Educational Rights and Privacy Act (FERPA) of 1974), including student academic, disciplinary, and financial records.

ii. Current, former, and prospective employees, including employment, pay, benefits data, and other personnel information.

iii. Donors, potential donors, Clinics and other University clinic clients, library patrons.

Other categories of confidential information include:

iv. Research information related to a forthcoming or pending patent application.

v. Certain University business operations, finances, legal matters, or other operations of a particularly sensitive nature.

vi. Information security data, including passwords. Information about security-related incidents.

d. **Highly Confidential**

This classification covers sensitive information which, if it becomes available to unauthorized users, creates risk for identity theft and therefore requires notification of affected individuals. This information includes Social Security Numbers, bank account numbers, credit card numbers, and driver's license numbers.

Summary Table

	Public	**Internal**	**Confidential**	**Highly Confidential**
Example	Schedule of Classes	Memos and minutes	Academic records	SSN
Access	Minimal controls to prevent unauthorized modification/ deletion	Determined by provider/sender	Limited based upon need to know, named users only, training and confidentiality agreement required	Provide access only when no alternative exists. Treat as toxic. Named users only, training and confidentiality agreement required

	Public	Internal	Confidential	Highly Confidential
Use	Post as needed	Determined by provider/sender	No posting, limited reporting and copying	Use only when no alternative exist. Treat as toxic. No posting, limited reporting and copying
Transmission	Minimal controls to prevent unauthorized modification	Determined by provider/sender	Confidential envelope; encrypted transmission	Hand deliver; encrypted transmission
Storage	Minimal controls to prevent unauthorized modification	Determined by provider/sender	Locked private office or cabinets; secure server and mainframe rooms ; secure backup and storage tapes; encryption on laptops	Locked private office or cabinets; secure server and mainframe rooms ; secure backup and storage tapes; encryption on laptops
Destruction	No Controls	Determined by provider/sender	Shred paper; securely delete files, wipe media	Shred paper; securely delete files, wipe media

Roles & Responsibilities

a. **Information Stewards**

Stewards are members of the University community who have primary responsibility for particular information. One becomes a Steward either by designation or by virtue of having acquired, developed, or created information resources for which no other party has stewardship. For example, the Office of Student Records is the Steward of student data; Human Resources is the Steward of employee data; Institutional Advancement is the Steward of donor data. Faculty are the Stewards of their research and course materials; students are the Stewards of their own work.

The term Steward as used here does not imply ownership in any legal sense, for example, as holder of a copyright or patent. Stewards have all responsibilities of Users (see next section). In addition, they are responsible for the following:

i. Establishing supplemental security policies and procedures. Stewards may establish specific information security policies and procedures for their information where appropriate. Stewards are responsible for the procedures related to the creation, retention, distribution and disposal of information. These procedures must be consistent with this Policy, as well as with other University policies, contractual relationships, and laws. Stewards may impose additional requirements that enhance security.

ii. Assigning classifications and marking information. Stewards are responsible for determining the classification of their information and any specific information handling requirements that go beyond this Policy, particularly as may be imposed by confidentiality agreements with third parties. Information that is Confidential or Highly Confidential shall be marked as such when it is presented or distributed to Users. Additional markings specifying handling and distribution requirements may be added.

iii. Determining authorizations. Stewards determine who is authorized to have access to their information. Stewards shall manage the list of all users who are granted access. The IT department will maintain access to data and make these records available for audit upon request.

iv. Training. Stewards of Confidential and/or Highly Confidential information shall ensure the development/compilation and delivery of appropriate training on security policies and procedures to be completed by users prior to being granted access to the information. Third party resources and services may be used. Stewards or their designees shall keep records of required training completion by users.

v. Confidentiality Agreement. Stewards of Confidential and/or Highly Confidential Information shall ensure that users sign an appropriate confidentiality agreement prior to being granted access. All confidentiality agreements must be reviewed and approved by University General Counsel.

vi. Periodic review of access and/or Termination of access. Stewards must terminate access to Confidential and/or Highly Confidential information resources in a timely manner when a User has changed roles or left the University. Access privileges should also be reviewed periodically to ensure accuracy.

b. **Information Users**

All members of the University community are "Users" of Loyola's information resources, even if they do not have responsibility for managing the resources. Users are responsible for

protecting information resources to which they have access. They shall follow the information security practices described in this policy, as well as any other information security practices specified by an information Steward and/or other information-related policies, including but not limited to the University's FERPA compliance policy, the Technology Resources Appropriate Use Policy, and Network Security Policy.

c. **Information Technology Security (ITS) Coordinator**

The ITS Coordinator manages the efforts of ITS and other University personnel to maintain and improve information security at Loyola. On behalf of the Vice Provost for Information Technology, the Security Coordinator is charged with taking steps to ensure compliance with this policy across the University, including assisting with training and development of technical and procedural solutions. The Security Coordinator also coordinates the ITS response to information security incidents.

d. **Information Technology Management Team** (ITMT)

The ITMT - Client Services, Computer Network Services, Telecommunication, and Distributed Systems, Information Management - must ensure ongoing compliance with this policy as they review new and continuing ITS initiatives.

e. **University Police**

The University Police is responsible for working with Information Technology in response to information security incidents in which a crime may have been committed. University Police shall conduct an investigation and prepare a report for the appropriate authorities, or provide support to authorities conducting their own investigation(s). **Risk management**

Risk Management will work with Information Technology, University Police, Internal Audit and appropriate insurance carriers to assist with investigations and reporting of incidents as required by law and to seek recovery of financial losses due to security breaches and other issues that may arise.

f. **Internal Auditor**

The Loyola Internal Auditor reviews Loyola information security practices and recommends appropriate controls to mitigate the risk of inappropriate information access and/or use.

g. **General Counsel**

The University General Counsel's office may provide guidance regarding laws applicable to Loyola information security policies and procedures. The office also reviews confidentiality agreements, this policy and proposed revisions for clarity and conformity with best practice.

h. **Third Parties**

Third parties with whom Loyola exchanges or entrusts Confidential and/or Highly Confidential information should provide the University with documentation of sound information security practices prior to any release of Confidential and/or Highly Confidential information. Information technology must approve all transmission methods for which confidential and/or Highly Confidential data is exchanged.

Acceptable Use

Loyola computer and network systems are intended for use in College-related research, instruction, learning, enrichment, and administrative activities.

Refer to Policy ‘GEN01-01 Computing Use’ for the details of the Acceptable Use Policy.

Access Controls

The University has developed processes for identity management purposes. These Processes manage the addition, modification and deletion of specific vendor and mainframe accounts and the roles and privileges assigned to account holders. In order to access these resources on the University network, faculty, staff, students, alumni and guest must first have their demographic and biographic information entered into the University’s computer system. Once an acceptable profile has been established within the system, specific access will be granted for the User and the User will be assigned one or more roles (e.g. student, employee) based on the profile. Users are assigned the appropriate set of privileges based on their role(s) at the University.
A University Steward must sponsor and approve any person who is requesting guest account privileges. Guest accounts are created after the guest’s demographic and biographic information is obtained. All guest accounts are created with an expiration date when available and these accounts become deactivated once the expiration date has passed. Use of shared or generic accounts should be avoided whenever possible.

Passwords

All computer devices that access Loyola’s network except for general public information applications (www.loyno.edu) should be password protected. This includes but is not limited to:

LORA,
EMAIL
Mainframe
PC’s
Handheld devices that receive email
Servers

Passwords should be unique, complex (if possible containing upper/lower letters, numeric and special characters) and changed on a regular basis.

Forgotten Passwords

In the event that a password is forgotten:

- Only authorized, full time employees of the Loyola University may reset passwords.
- Where available a self service reset process will be used by the end user.
- No passwords will be changed on behalf of a computer user without positive identification such as a Campus ID card.
- If the user cannot come to the Help Desk, with proper identification, then resets may be performed over the phone after alternate verification of the user's identity.
- If technically possible, the new password that is reset on behalf of a computer user will be set to expire upon first use by the user, who will then be prompted to choose a new password.

Physical Security

Users must not store passwords on personal computers in an unencrypted fashion or on paper. Users are responsible for securing their Electronic Resources against unauthorized access when left unattended. Users are responsible for the physical security of their computers and Electronic Resources in their office and on-campus living areas. Doors must be locked to protect these resources when an area will be unattended for any period of time. Users with portable devices such as PDAs and laptop computers must be especially careful and attentive in protecting and securing these devices. It is the responsibility of the User to report any policy violations to the Department Heads or Managers for the specific information resource or the University's Information Security Officers.

Training

Users must complete training, as designated and recorded by the Information Steward, prior to being granted access to Confidential and/or Highly Confidential information. An annual review of all security measures should be conducted.

Confidentiality Agreement

Users with access to Confidential and/or Highly Confidential information must acknowledge that they have read this agreement prior to being granted access to the Information assets of the University.

All Third party vendors must sign a Confidentiality Agreement prior to conducting business with Loyola when Confidential and/or Highly Confidential information is exchanged.

Privacy

Loyola University collects and retains information and data about its students, employees, alumni and friends in support of the teaching, learning, research and service mission of the University. The University is committed to protecting and maintaining the privacy of this information. Access to University information is restricted to faculty, administrators and staff who need that information in order to perform the duties of their position. Employees with access to this information may use it only for the purposes of fulfilling the duties and responsibilities of their positions and in accordance with applicable privacy laws.
In order to maintain and protect this privacy it is incumbent upon every person within the University system to abide by the rules set forth in this policy.

Storage of data

1. Centrally stored data will be maintained using the most secure security procedures available. (Firewall security, encrypted servers, etc)

2. Personally stored data. It is recommended that no one store confidential of highly confidential information on any personal storage devices. But if it does become necessary the following rules must be followed:

a. ITStor is a network storage area used to store information shared between users and departments. It is secure and not intended to be used for workstation/personal computer backup purposes. Security is maintained at the user level.

b. All removable media should be encrypted with either hardware or software encryption. Passwords should be complex and physical security should be maintained at all times.

c. Individual computers (laptops) should use either hardware or software encryption.

d. Paper reports should never contain highly confidential data unless required by government agency receiving the report. All reports containing information ranked above public use should be maintained in physically secure areas and/or transported.

e. Use only approved secure carriers for mail delivery.

3. Cloud-based storage. Cloud-based storage, such as Google Drive, DropBox, Box, etc. should not be utilized to store university data. Such storage mechanisms do not provide for data encryption and data stored with such services cannot be considered secure.

4. Transmitted data.

    a. All data transmissions should be performed using secure SSL encryption websites or FTP secure services. If you have any questions about the security of a transmission please contact the Help Desk prior to performing the transmission. Under no circumstances should confidential of highly confidential data be transmitted or delivered via email attachment.

5. Vendor/3rd party maintained applications.

    a. All applications maintained offsite should be reviewed by IT prior to any data being collected or sent offsite.

Data Destruction

1. PC's, Servers and other computer equipment should be wiped clean by a certified vendor prior to disposal or donation to any organization. Refer to 'CSTECH01-01 Desktop data security Policy' for more information.

2. CD, DVD's and Thumb drives should be destroyed using proper approved techniques.

3. Paper should be destroyed using the University's contracted service. If you need access to a destruction bin please contact Physical Plant.

Risk Management

Periodically, a risk assessment is conducted by external auditors to review access policies, procedures and controls. The audit ensures that only authorized users can gain access to the University's network and systems. In addition, the audit will review IT operations, general security, application controls, and database, network and system administration.

Change Management

It is the responsibility of the IT department to make any change to the system software or hardware based on acceptable approved work request or system malfunction. These changes will be made in accordance with the Programming Change Control Procedures (IMGMT01-01), the INTEL Server Change Management Policy (OPER-0202) and Change Control Policy for System and Network Updates (OPER01-05), .

Incident Reporting

Users shall report known or suspected compromises of University information security to the IT Help Desk or Risk Management. The ITS Security Coordinator will inform the appropriate departments and, if it appears that a crime may have been committed, the University Police. In such cases, a police incident report should be created prior to the start of investigation. ITS detailed investigation reports must be shared with the University Police and appropriate executive officers only, when allowed by law, with only general status information reported, if appropriate, to the broader community. Non-criminal incidents will be treated as Confidential unless information subject to Louisiana law has been compromised. In this case, affected individuals will be informed.

The ITS Security Coordinator shall coordinate the efforts of all involved parties to investigate the incident. The Coordinator shall provide frequent status reports to the Vice President for Information Technology and other executive officers, as appropriate, and submit a complete incident report to the Vice President for Information Technology upon completion of the investigation when allowed by law.

Enforcement

Members of the University community who knowingly violate this policy may be subject to disciplinary action and/or removal of access to all Information Assets. Members of the University community are responsible for familiarity with this policy.

Contingency Planning

It is the responsibility of the University to develop and maintain a contingency plan in the event of an emergency or loss of computer services. This plan requires that all critical computer services be available, if necessary at an offsite location (Disaster recovery Site) in the event of the production environment being unavailable for use.

Disaster recovery

Loyola University maintains a strong Disaster recovery program. To ensure that all computer and University operations can continue in the event of a disaster, a recovery contract is maintained to provide computer equipment and operation space in locations outside of the Louisiana area. The recovery plan is executed/ tested, annually to ensure the reliability of the service.

Back up and offsite storage

It is the goal of the IT Vice Provost to ensure that all computer systems are backed up properly and data is maintained in the event of a disaster. Please refer to the following policies for more information:

OPER01-02 Mainframe Back Up Policy

OPER01-03 AIX/Intel Tape Back Up

OPER02-01 Intel Server Back Up and Recovery Policy

It is the responsibility of each user to ensure that proper backups are taken of their personal computers. The IT department has made CrashPlan Pro (CPP) available to all Faculty and Staff who request it to maintain data backups of all user files stored on their PC.

Review Cycle

This Policy will be reviewed and updated on an annual basis. More frequent updates will occur as required by changes in the University's computing and information resources based on the Recommendations of the Assistant Vice Presidents of Information Technology, the Risk Management Committee or Information Security Sub-Committee of the Information Technology Advisory Council.
Refer to 'CSTECH01-01 Desktop Data Security Policy' for more details.

Glossary

1. Information assets - Information in any form, recorded on any media. Such assets include data, images, text, software, and voice recordings, in digital or analog form, stored on hardware, paper or other storage media.

2. Acceptable Use - The proper and appropriate use of the University's Electronic Resources in support of the teaching, learning, research and service missions of the University.

3. Access Control - The mechanism for limiting access to Information Resources to those users who are entitled to them.

4. Availability - Ensuring timely and reliable access to and use of information; the *loss of availability* is the disruption of access to or use of information or an information system.

5. Confidential Information - Sensitive, high-risk information about an individual or the University including, but not limited to, student academic history, student discipline, student financial records, social security numbers, employment and benefit information, alumni giving, research information, user passwords, privileged communications, etc.

6. Data Classification - The conscious decision to assign a level of sensitivity to data as it is being created, amended, enhanced, stored, or transmitted.

7. Data Integrity - The correctness, completeness and validity of the information being maintained.

8. Data Steward - The individual responsible for the accuracy, integrity, consistency and relevancy of specific information within their assigned areas. The steward may be responsible for data managed and stored within a specific module of the Mainframe SIS system, the University's web sites and any other repository for University data.

9. Disaster Recovery - The ability of the University to respond to a disaster or an interruption of services by implementing a Disaster Recovery plan to stabilize and restore the critical functions.

10. Intranet – internal network isolated within the University security system intended for internal use only.

11. ITS – Information Technology Security.

12. ITMT – Information Technology management Team primarily made up of the management staff of the Information Management Department.

13. LORA – Loyola Online Records Access. Primary tool for students to access schedules, course information etc.

14. Removable media – Thumb drive, CDs, and DVDs.