Security Policy for Technology Professionals

Policy Title:
Security Policy for Technology Professionals

Responsible Executive(s):
Chief Information Security Officer

Responsible Office(s):
University Information Security Officer

Contact(s):
If you have questions about this policy, please contact the University Information Security Office.

I. Policy Statement

This policy covers all of Loyola University Chicago's computing, networking, telephony and information resources. All members of the University community share the responsibility for protecting information resources for which they have access or custodianship.

The purpose of this policy is to establish the University's approach to information security and to establish procedures that will help identify and prevent compromises of information around the University's computing, networking, telephony and information resources, as well as to create a secure baseline standard for the University's computing, networking, telephony and information resources.

II. Definitions

Server: a software program, or the computer on which that program runs, that provides a service to client software running on the same computer or other computers on a network.

III. Policy

Individuals Covered

This policy applies to all information technology professionals employed by the University who are responsible for the installation, management, and maintenance of computing, networking, telephony, and information resources. These persons include students, faculty, staff, persons retained to perform University work, and any other person extended access and use privileges by the University given the availability of these resources and services, and in accordance with university contractual agreements and obligations.

Systems and Resources Covered

This policy covers all computing, networking, telephony and information resources procured through, operated or contracted by the University. This policy also covers any computing device connecting to and utilizing University information resources. Such resources include computing and networking systems including those that connect to the University telecommunications infrastructure, other computer hardware, software, databases, support personnel and services, physical facilities, and communications systems and services. Authorized support personnel for high security systems are outlined in the ITS Roles and Responsibilities Matrix and Audit Calendar.

Information Classification & Protection

In order to ensure that information about members of the University community is properly protected, all information will be classified in accordance with the Data Classification Policy. Information that is classified as Loyola Protected or Loyola Sensitive data will receive additional protections as described in the Personally Identifiable Information (PII) Protection Policies. Data deemed PCI-DSS relevant must comply with all PCI-DSS requirements as outlined by the PCI Data Security Standard Version 3.2. All Personal Health Information (PHI) must be protected or properly redacted as outlined in the HIPAA Privacy Rule.

User Training and Awareness

Effective information security requires a high level of participation from all members of the University and all must be well informed of their responsibilities. To facilitate this, information security awareness materials and training will be provided to the Loyola community in accordance with the ITS Security Awareness Policy.

Physical and Environmental Security

Centralized computer facilities will be protected in physically secure locations with controlled access, in accordance to the ITS Password Standard. They will also have appropriate environmental safeguards. Departmental computers housing Loyola Sensitive or Loyola Public data may require physical and environmental security safeguards. All servers containing Loyola Protected data must be housed in an approved ITS data center.

Incident Response

Information security incidents have the potential to negatively impact members of the University community and to harm the University's reputation. Therefore, it is important that all information security incidents are handled confidentially and appropriately. All information security incidents will be handled in accordance with the ITS Computer Security Standard.

Risk Assessment

Security incidents are more likely to occur when there are unknown and unaddressed risks and vulnerabilities in information systems. Therefore, risk assessments will be conducted in accordance with the ITS Risk Assessment Process. In addition, the IT

Security Team will periodically perform vulnerability assessments, per the ITS Router and Switch Security Standard.

Network and Computer Security

All networking devices procured through, operated or contracted by the University will be configured in accordance with the ITS Router and Switch Security Standard, the ITS Network Firewall Policy, or the ITS Wireless Access Point Policy, depending on the type of device that it is.

All workstations, desktops and laptops procured through, operated or contracted by the University will be configured in accordance with the ITS Computer Security Standard and the ITS Password Standard.

All servers procured through, operated or contracted by the University will be configured in accordance with the ITS Computer Security Standard and the ITS Password Standard.

Antivirus

Viruses and other malicious programs can compromise the confidentiality, integrity, and availability of information resources. All systems connected to University networks shall abide by the ITS Antivirus Policy.

Password Security

All workstations, desktops and laptops procured through, operated or contracted by the University will be configured in accordance with the ITS Password Standard.

Antivirus

Viruses and other malicious programs can compromise the confidentiality, integrity, and availability of information resources. All systems connected to university networks shall abide by the ITS Antivirus Policy.

Key Management

All systems that store Loyola Protected data will encrypt said data using appropriate encryption techniques, as defined within the Encryption Policy. This policy requires the use of private keys to encrypt the data.

Individuals who, because of their job function, are responsible for using a private key will be designated as “key custodians”. No key custodian will have knowledge of a majority of the private keys.

Any private keys created during the encryption process will be maintained via a key management procedure specific to that system. This procedure is determined by the key custodians, and must include the following items:

- Require split knowledge and dual control of private keys, so that at least two key custodians are required to install a single key component or enter a passphrase, for the generation or installation of an encrypting private key.

- An individual who is not serving as a key custodian must be present during the installation of the private key to witness the installation and sign the ITS Key Management Log. The witness will then submit the ITS Key Management Log to the UISO.
- Require that key custodians sign the ITS Key Management Responsibilities Form, indicating they understand their key management procedures and responsibilities.
- Restrict private keys to the fewest number of key custodians possible
- Store private keys securely in the fewest possible locations
- Generate strong keys and securely distribute them to the appropriate key custodians
- Change private keys at least annually, or as deemed necessary, whichever comes first.
- Replace all known or suspected compromised private keys immediately.
- Securely destroy all private keys that are changed and re-encrypt the data with new private keys.

Log Management

System logs are required to enable effective troubleshooting of system problems and are a required component of the incident response process. All systems that store, transmit or process Loyola Protected data shall abide by the ITS Log Management Standard.

Policy Adherence

Failure to follow this policy can result in disciplinary action as provided in the Employee Staff Handbook, Student Worker Employment Guide, and Faculty Handbook. Disciplinary action for not following this policy may include termination, as provided in the applicable handbook or employment guide.

Exceptions

Exceptions to this policy will be handled on a case-by-case basis and reviewed and approved by the University Information Security Office.

Review

This policy, and all policies, standards, handbooks and supporting materials contained within, will be reviewed by the UISO on an annual basis.

Emergencies

In emergency cases, actions may be taken by the Incident Response Team in accordance with the procedures in the ITS Incident Response Handbook. These actions may include rendering systems inaccessible.

IV. Related Documents and Forms

Not applicable.

V. Roles and Responsibilities

Chief Information Security Officer	Enforcing the Security Policy at the University by setting the necessary requirements.

VI. Related Policies

Please see below for additional related policies:

- ITS Password Standard
- ITS Security Awareness Policy
- Data Classification Policy
- ITS Incident Response Handbook
- Employee Staff Handbook
- Student Worker Employment Guide
- Faculty Handbook
- ITS Log Management Standard
- Encryption Policy
- Antivirus Policy
- Computer Security Standard
- Router and Switch Security Standard
- Network Firewall Policy
- Wireless Access Point Policy

Approval Authority:	ITESC	**Approval Date:**	June 17th, 2015
Review Authority:	Jim Pardonek	**Review Date:**	June 14st, 2024
Responsible Office:	UISO	**Contact:**	datasecurity@luc.edu