Security Policy

Policy Title:
Security Policy

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. In addition, please note that this policy covers all IoT devices.

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 persons accessing and using computing, networking, telephony, and information resources through any facility of the University. 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. There are additional requirements for information technology professionals employed by the University who install, manage, and maintain computing, networking, telephony, and information resources. These individuals should reference:

https://www.luc.edu/its/aboutits/itspoliciesguidelines/security_policy.shtml. Activities related to teaching and learning are excepted provided they are segmented from the general university network and do not violate and State of Federal regulations.

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.

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. All Personal Health Information (PHI) must be protected or properly redacted as outlined in the HIPAA Privacy Rule. Individuals and departments that require the acceptance of credit card payments on behalf of Loyola University Chicago will have to adhere to additional requirements and will need to contact Loyola Cash Management for assistance.

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

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. Any potential incident should be reported to the University Information Security Office.

Network and Computer Security

All devices connected to the university network must be approved by Information Technology Services prior to connecting via manual or automated means.

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.

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.

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

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