Computer Security Standard

Policy Title:
Computer Security Standard

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 standard applies to all computers, defined as any workstation, desktop or laptops that are:

- Owned or managed by Loyola University Chicago
- Connected to Loyola University Chicago networks
- Connected to Loyola University Chicago resources or services
- Storing Loyola University Chicago data

The owner of a computer may use it at his or her discretion; however, once that computer is connected to the Loyola University network or is used to store university data, it is subject to applicable laws and regulations, and to Loyola University policies.

The purpose of this document is to establish standards for the base configuration of Loyola University computers. Effective implementation of this standard will minimize security incidents involving University resources.

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

This document is broken up into two sections: Baseline Standards and High Security.

II. Definitions

High Security Systems: Servers, applications, or network computers that store, process or transmit Loyola Protected Data, per the Data Classification Policy.

Service Accounts: User accounts that are required by applications as part of their normal function and operation. These accounts are not used by users to login interactively.

III. Policy

The following sections must be adhered to by the user of the computer.

Baseline Standards

- Computers must use a vendor supported operating system that currently receives vendor security updates and technical support. Security updates patch vulnerabilities that may be exploited by malware and help keep users and their data safer. Unsupported operating systems will not be allowed to connect to the network.
- Users must lock their computer or logout prior to leaving the area to prevent unauthorized access.
- All user accounts must have a unique local profile associated with their account.
- The University does not allow the use of shared local profiles, when logging in to a Loyola workstation.
- Computers will comply with the ITS Password Standard.
- Computers will comply with the ITS Antivirus Standard.
- Computers will comply with the Electronic Security of Loyola Protected Data & Loyola Sensitive Data Policy.
- Personal firewalls will be enabled on the computer and will filter inbound traffic to the host with a “deny all” policy.
- Users will implement anti-spyware on their computer.
- Users will disable unneeded services, e.g. SMTP or FTP if enabled by default by the operating system.
- Users will regularly check and install all critical and security patches for the operating system and applications as soon as possible, no later than within 30 days of their release.

High Security Standard

All computers procured through, operated, or contracted by the University and connected to, or interacting with, a high security network zone, as defined in the ITS Network Firewall Policy, or store Loyola Protected Data, must adhere to the following rules in addition to the Baseline Standard:

- The operating system will be configured in accordance with approved Information Security guidelines, as referenced in the Appendix.
- Users will enable a password-protecting screen saver on their desktop that will lock their desktop after 15 minutes of inactivity.
- Users will not login using generic, shared or service accounts.
- Users will ensure monitors are positioned in such a way so that it restricts the viewing of Protected Data to anyone but the operator.
- Personal firewalls must not be altered by users.

- The computer will not function as a server (e.g., will not provide file shares, web, ftp or peer-to-peer applications).
- The computer will not access high security systems or networks using wireless technology except via VPN.
- Computers that access high security systems will enable all security and access logging in accordance with the ITS Log Management Standard.
- Authorization for remote access to computers will be submitted, with valid business justifications, to the Chief Information Security Officer (CISO) for approval.
- All approved remote access will comply with the ITS Access Control Policy.
- All approved remote access techniques will be encrypted between the computer and the remote machine.
- Trusted zones may be explicitly enabled in browsers for specific web sites on an as needed basis.
- Change vendor supplied defaults and remove or disable unnecessary default accounts before a computer is installed on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).
- All computers will be properly sanitized prior to their disposal or decommissioning, per the Disposal of Loyola Protected Data & Loyola Sensitive Data Policy.

All computers that are capable, shall contain a login banner that displays the following content:

"This computer and network are provided for use by authorized members of the Loyola community. Use of this computer and network are subject to all applicable Loyola policies, including Information Technology Services policies and any applicable Loyola Handbooks. Any use of this computer or network constitutes acknowledgment that the user is subject to all applicable policies. Any other use is prohibited. Users of any networked system, including this computer, should be aware that due to the nature of electronic communications, any information conveyed via a computer, or a network may not be private. Sensitive communications should be encrypted or communicated via an alternative method."

IV. Related Documents and Forms

Not applicable.

V. Roles and Responsibilities

Chief Information Security Officer	Enforcing the Computer Security Standard at the University by setting the necessary requirements

VI. Related Policies

Please see below for additional related policies:

- Security Policy
- Disposal of Loyola Protected Data & Loyola Sensitive Data Policy
- Electronic Security of Loyola Protected Data & Loyola Sensitive Data Policy
- Access Control Policy
- ITS Antivirus Policy
- Incident Response Plan
- Log Management Standard
- Network Firewall Standard
- Password Standard

Approval Authority:	ITESC	**Approval Date:**	June 7th, 2017
Review Authority:	Jim Pardonek	**Review Date:**	June 14th, 2024
Responsible Office:	UISO	**Contact:**	datasecurity@luc.edu