Supported Operating Systems Standard

Policy Title:
Supported Operating Systems Standard

Responsible Executive(s):
Chief Information Security Officer

Responsible Office(s):
University Information Security Office

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

I. Policy Statement

Information Technology Services (ITS) will only provide support or grant network access for the versions of Operating Systems that meet the security requirements for a safe and secure computing environment. This document is intended to provide information on what operating systems are acceptable for use at all campuses of Loyola University Chicago.

II. Definitions

Not applicable.

III. Policy

Loyola Owned Computers

The current Windows operating system that is installed and supported on all Loyola-owned desktops and laptops is Windows 10. Windows 10 is installed and maintained by ITS or by specific departmental IT departments. ITS maintains copies of the Windows Operating System licensed for Loyola University Chicago owned computers only (not personally owned or student computers). Windows 11 may be installed on some computers.

Personally Owned Windows Computers

Students, faculty and staff, are all required to be registered on Loyola wireless networks and wired networks in the residence halls. Loyola provides free wireless access for all devices to all students, faculty, and staff. If your computer is not fully updated, is

running an "out of support" operating system, is missing the appropriate anti-virus, or has peer-to-peer file sharing programs installed, you will not be allowed onto our network. Supported Windows operating systems include:

- Windows 10
- Windows 11
- Windows 8
- Windows 7
- Windows Vista

Deprecated Versions of Windows

Microsoft no longer provides security updates or technical support for the following desktop operating systems.

- Windows XP
- Windows 8
- Windows 7
- Windows Vista

Security updates patch vulnerabilities that may be exploited by malware and help keep users and their data safer. PCs running deprecated versions of Windows, should not be considered to be protected, and it is important that you migrate to a current supported operating system so you can receive regular security updates to protect your computer from malicious attacks.

If you have equipment that requires a deprecated version of Windows to function, such as scientific instrumentation or scanners, please contact the ITS Helpdesk. We will work with you to discuss upgrade options or make accommodations for your computer that will provide an additional level of security and keep the computer safe.

Macintosh OS X

Information Technology Services (ITS) provides limited support for Apple computers regardless if purchased individually or with university funding.

Supported versions of MacOS are:

- macOS 14 (Sonoma)
- macOS 13 (Ventura)
- macOS 12 (Monterey)

Loyola does not maintain a licensing agreement with Apple. As a result, ITS does not distribute MacOS to Loyola users. Users who want to install MacOS on their computers must purchase both media and license from the App Store.

- Operating Systems other than MacOS (for example, Windows via Parallels or Boot Camp) running on Apple computer hardware are unsupported.
- Any MacOS running on hardware other Apple computer hardware is unsupported.

Tablets, PDAs and Smartphones

- iOS 15 and above
- Android 12 (Snow Cone) and above

Linux Operating Systems

- Loyola will provide best efforts to permit access for Linux operating systems and cannot guarantee access.
- Most standard distributions will work.

IV. Related Documents and Forms

Not applicable.

V. Roles and Responsibilities

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

VI. Related Policies

Please see below for additional related policies:

- Security Policy

Approval Authority:	ITESC	**Approval Date:**	September 16th, 2014
Review Authority:	Jim Pardonek	**Review Date:**	July 7th, 2024
Responsible Office:	UISO	**Contact:**	datasecurity@luc.edu