Simmons
UNIVERSITY

Endpoint Guidelines

Technology

Last updated: 2/10/2025

Table of Contents

Introduction

This document describes the guidelines used by the Technology department to manage the allocation and replacement of the desktop computers, laptop computers, virtual client devices, and mobile devices (collectively, *endpoints*) that are purchased and owned by the University.

Endpoints are used...

- ➔ by individual faculty and staff
- ➔ in shared workspaces and offices for part-time and student staff
- ➔ in computer labs, classrooms, event spaces, and meeting rooms
- ➔ in general access carrels, library spaces, study rooms, and kiosks
- ➔ for temporary computing needs

Endpoints are assigned to individual faculty and staff based on job function requirements. These guidelines are in place to enable faculty and staff to perform their roles while also maximizing the useful life of each endpoint and the efficiency of University resources.

Manufacturers update their endpoint models periodically. Technology will negotiate new standard configurations in order to maintain consistency, performance, price, and suitability for the University. Technology will document changes in the appendices of this document.

Default assigned endpoints:

- ➔ Staff = Laptop running Windows, macOS or virtual client device
- ➔ Faculty = Laptop running Windows or macOS

Additional notes:

- ❖ Based on job requirements, enhanced hardware configuration may be deployed with proper justification from management and—in some cases—approval from a University Leadership Team member.
- ❖ Choice of operating system should be approved by the manager.

Overview

Definitions

- **Endpoint**: a desktop or laptop computer, virtual client device, or mobile device running an operating system (Android, Chrome OS, iOS, iPadOS, macOS, Windows). Technology sets the replacement guidelines that define the level of deployment and support services for users throughout the University.

- **Peripheral**: a device connected to an endpoint to provide communication—such as input and output—or auxiliary functions.

- **Instrument**: a device connected to an endpoint that provides specific data especially for measuring and recording.

Goals

- Provide endpoint hardware and software that supports teaching, learning, and administration
- Provide an appropriate and manageable variety of standard endpoint configurations to balance cost and need
- Maintain a streamlined and predictable process for replacing endpoints

Scope

- Faculty, staff, shared, and loaner endpoints
- Classroom, computer lab, and general access endpoints
- Updating operating systems to current, tested, and approved versions
- Upgrading software as needed to be compatible with new operating systems and both academic and administrative needs
- Replacing end-of-life hardware with up-to-date hardware configurations

Community Benefits

- Enhanced student experience through an improved learning environment
- Enhanced faculty and staff experience through higher levels of performance and support
- Improved security and reliability through internal, automated software updates
- Reduced total cost of ownership of the University's endpoint fleet by replacing poor-performing hardware with faster, more powerful models

Individual Endpoint Eligibility

- Full-time faculty and staff
- Part-time faculty and staff working 20 hours per week or more
- Contingent staff with specific computing needs to perform their job function

Guidelines

1. Lifecycle Management

1.1. Technology will order, receive, and maintain all endpoints that are purchased by the University and are considered University-owned assets.

1.2. Support for all endpoints that are considered University-owned will be provided by the Technology Service Desk. All information about support services, including hours and contacts, will be provided at servicedesk.simmons.edu.

1.3. Endpoints will be replaced on a cycle determined by the Finance and Provost's Offices based on academic need, financial resources, and the University's strategic plans.

1.4. At the end of each cycle, Technology will conduct a fleet assessment and recommend options for approval by the Finance and Provost's Offices. The faculty and staff replacement cycle may be separate from the classroom, lab, and general access replacement cycle—which serves a different purpose.

1.5. Replacement endpoints will follow these guidelines:

§	Risks and Issues	Guideline
1	Employees may store important, work-related data locally on the endpoint.	Technology will transfer all appropriate data from the legacy endpoint to the replacement endpoint.
2	Employees need time with the replacement endpoint to ensure all data has been properly transferred from the legacy endpoint.	Technology will hold the legacy endpoint for two (2) weeks to ensure no further data is needed.
3	Legacy endpoints may no longer have useful life or their condition is poor.	Legacy endpoints will be returned to Technology for a useful life assessment.

1.6. When a legacy endpoint or accessory still has useful life, Technology will verify that all of its components are in good working condition and assign it as gently-used inventory.

1.7. When a legacy endpoint or accessory no longer has useful life, Technology will ensure it is donated, recycled, or disposed of in a responsible manner through a variety of different programs.

1.8. Before donating, recycling, disposing, or repurposing an endpoint or related accessories, Technology will wipe its hard drive in a secure manner in order to comply with Massachusetts General Law Chapter 93H and its regulations 201 CMR 17.00.

1.9. The University does not offer legacy endpoints for personal purchase. Employees may purchase equipment at discounted rates through vendor purchasing programs.

1.10. When an endpoint fails or needs an urgent or unplanned replacement, Technology will determine the best approach for the situation. This may include alternatives for

replacement or issuing gently-used inventory.

1.11. Endpoints shall not be exchanged, traded, or reassigned without notification to and approval of Technology. When an endpoint needs to be moved from its original location, Technology is informed in order to update inventory records.

1.12. Endpoints deployed off-campus will be configured with a local user account for access.

1.13. Technology may redeploy, relocate, or retrieve endpoints as academic needs change.

1.14. Technology is notified when employees leave their position and will contact their manager to discuss the disposition of all assigned endpoints. Managers are responsible for collecting endpoints from outgoing employees and returning them to Technology. Unreturned endpoints will be included in Technology weekly audit reports.

1.15. Technology will conduct an annual review of endpoints in department shared spaces to verify they still meet the department's needs and maximum number of concurrent employees for the space.

2. Local Department Management

In unique situations, departmental and lab managers will partner with Technology to manage endpoints embedded in classrooms and labs. Technology is ultimately responsible for the support and security of these endpoints.

2.1. Co-managed endpoints will follow these guidelines:

§	Risks and Issues	Guideline
1	Certain categories of information are classified as high risk, either because the exposure of this information can cause harm or because the information is specifically protected under law or under contract.	Comply with the University's Acceptable Use Policy and Information Security Policy.
2	Technology must know the location of endpoints to assist with hardware and software repairs. Technology must report missing endpoints and their last known location to Public Safety.	Local Department and lab administrators will coordinate with Technology to move, replace, or locate hardware components. This includes the installation of aftermarket parts and components.
3	To prevent unscheduled downtime or loss of productivity due to system or component failure, preventative maintenance and regular cleanings need to be performed to extend or maintain the life of an endpoint.	Perform cleaning and routine preventative maintenance. This includes applying patch updates and performing periodic reboots.
4	Desktops and laptops must be joined to the University's Active Directory domain to take advantage of many Technology offerings such as Microsoft Office (Word, PowerPoint, Excel), departmental file shares, patch management, single sign-on, etc. Exceptions to some settings that Technology applies to domain-joined endpoints can be added to prevent any departmental impact.	All desktops and laptops must be joined to the University's Active Directory domain.

5	Endpoints will be configured to support Local Department and lab administrator requirements. Technology will develop change management procedures that support the needs of Local Departments and lab administrators while maintaining the integrity and security of the endpoint environment.	Technology will maintain or verify images and manage changes to all endpoints.
6	Technology must track issues related to endpoints. The Service Desk is the single point of contact and will triage requests within Technology.	Contact the Technology Service Desk to report hardware and software issues.

3. Funding

3.1. Funding for endpoints is determined on a yearly basis by the Chief Financial Officer and the Provost. If funding is suspended for the fiscal year, endpoint replacements will be suspended.

3.2. All endpoint purchases must be approved and acquired through Technology from the University's preferred vendors.

3.3. Grant-funded endpoints must be an approved purchase by the appropriate grant administrator before being acquired through Technology. These endpoints are considered University-owned assets.

3.4. All endpoints will be purchased with a limited hardware warranty of no less than three (≥3) years.

3.5. At the end of each fiscal year, Technology will conduct a review of the University's preferred vendors and verify they still meet academic needs, financial resources, and the University's strategic plans.

See Appendix B: Preferred Vendors for the current preferred Technology vendors.

3.6. Any endpoint purchased outside of Technology will be reported to the appropriate University Leadership Team member and may not be managed by Technology.

3.7. The University provides funding for one (1) endpoint hardware configuration bundle per benefited position, if the job duties of the position require an individual endpoint.

See Appendix C: Employee Eligibility for employee types that meet this guideline.

3.8. Eligible Non-Campus Based Employees will be provided one (1) laptop endpoint device and a multiport display adaptor for connecting to most external monitors.

See HR Non-Campus Based Employee Remote Policy

3.9. When an employee's configuration consists of more than one (>1) endpoint, Technology will be responsible for funding the replacement of one (1) endpoint. The need to replace and fund any additional endpoints will be assessed by the appropriate University

Leadership Team member.

3.10. When a non-benefited position requires a bundle configuration, the appropriate University Leadership Team member is responsible for confirming and approving the need. The University will provide funding for one (1) endpoint hardware configuration bundle per approved non-benefited employee.

3.11. When a department requires bundle configurations for a shared space used by part-time, student, or contingent employees, the appropriate University Leadership Team member is responsible for confirming and approving the need. The University will provide funding for desktop configuration bundles that satisfy the maximum number of concurrent scheduled employees in the department shared space.

3.12. When a department requires an enhanced bundle configuration for everyday operations, the appropriate University Leadership Team member is responsible for confirming and approving the need before the next budget cycle. Otherwise the cost difference between the standard offering and the upgraded bundle will be billed to the department.

3.13. Additional peripherals not included in a standard configuration bundle (see 4.6) will be funded by the department of the requestor and acquired through Technology or Technology-approved third-party vendors.

3.14. Software not found in the standard set of software will be funded by the department of the requestor and acquired through Technology.

3.15. Lost, stolen, or damaged endpoints may be covered by the Technology contingency repair budget. Technology may deny funding for the replacement of an endpoint if it is determined that the department or user did not follow the user responsibility guidelines.

3.16. Endpoints purchased for personal ownership using University funds (e.g. development funds) are considered personal assets and will not be managed by the University.

3.17. Endpoints deployed to off-campus employees (e.g. online faculty) will be shipped to and from campus using a preferred shipping vendor. Shipping labels will be funded and provided by Technology.

3.18. To request a disability accommodation, contact the Human Resources department. The University makes every effort to honor all disability accommodation requests. Requests can be responded to most effectively if received as far in advance as possible.

4. Hardware

4.1. Technology will maintain a set of standard endpoint hardware configuration bundles and assign endpoint bundles based on job function requirements.

4.2. Hardware configuration bundles are designed to be as versatile as possible to support all departments, job roles, and use types.

4.3. Enhanced configurations need approval from a hiring manager and—in some cases—a

University Leadership Team member.

4.4. Eligible full-time remote employees will receive a laptop and display adaptor without additional peripherals.

4.5. Hardware configuration bundles will be reviewed each time a new model of the same series is released by the manufacturer, or when a model series is discontinued.

§	Configuration Bundle	Justification	Cost	Approval
1	Virtual Client Device	Standard employee computer configuration	$450	N/A
2	Standard Desktop	Standard employee computer configuration	$900	N/A
3	Standard Laptop	Job function requires computing portability—including remote work	$1,300 - $1,600	Hiring Manager
5	Enhanced	Job function requires enhanced computing and graphics performance	$1,600+	University Leadership Team

See Appendix D: Standard Hardware Configuration Bundles for current bundles.

4.6. Hardware configuration bundles will include a set of approved peripherals.

§	Configuration Bundle	Peripherals
1	Desktop / Virtual Client Desktop	One (1) Monitor [may be built-in] One (1) Keyboard One (1) Mouse
2	Laptop	One (1) Video Adapter One (1) Monitor [optional] One (1) Keyboard [optional] One (1) Mouse [optional]

4.7. If an employee's department, job role, or employee type changes, any request for a new configuration bundle must be approved by the employee's manager and—in some cases—a University Leadership Team member.

4.8. Technology will maintain a fleet of loaner laptops and manage their circulation.

§	Loaner Type	Guideline
1	Short-term Loaner Laptop	Laptop loaned to a student or employee for no more than one (1) calendar week.
2	Long-term Loaner Laptop	Laptop loaned to an employee for more than one (1) calendar week and no more than one (1) academic term. Must be approved by the appropriate University Leadership Team member.

4.9. Classroom, Computer Lab, and General Access configurations will be designed to be as versatile as possible to support the broadest use by students from across the University.

5. Software

5.1. Technology will purchase and maintain a standard set of software for endpoints.

See Appendix E: Standard Software Configurations for current set.

5.2. Endpoints will be configured with a standard set of software intended for classroom, computer lab, and general access productivity computing.

5.3. Endpoints will be configured with a single operating system. Technology will evaluate options and provide manageable configurations for employees who need to run multiple operating systems.

5.4. In order to protect faculty, staff, and student data as well as the security of the University's network, endpoints will run a standard suite of security and system management software to include anti-virus, anti-malware, encryption, security patches, and endpoint management. This software is critical for asset management, software updates and remote support by Technology staff. The software also enables the University to comply with the Commonwealth of Massachusetts regulations regarding computer security and protection of sensitive information.

5.5. At the end of each cycle, Technology will conduct a review of the standard set of software and verify that it continues to meet academic needs, financial resources, and the University's strategic plans.

5.6. Requests for obtaining and packaging software not included in the standard suite will be made through Technology. It is a good practice to plan ahead if new software versions are released and changes to the curriculum are needed. Technology needs time to not only build the package, but to test it with the appropriate liaison within the department or a lab to ensure it meets requirements.

5.7. New software requests—including upgrades—must meet the following guidelines:

§	Risks and Issues	Guideline
1	Based on our academic calendar, there is a large spike in demand from all schools and departments for new software packages at the start of each semester.	There is an eight (8) week lead time for software packaging and deployment requests.

6. Training

Technology has made the following self-service tools available to all faculty, staff and students:

6.1. Self-guided training through https://learning.linkedin.com/.

6.2. Self-guided online videos covering specific user interface topics.

6.3. How-To Articles with tips, shortcuts, and explanations for commonly used features in the software through servicedesk.simmons.edu.

7. User Responsibilities

7.1. Users are responsible for meeting the following guidelines:

§	Risks and Issues	Guideline
1	Certain categories of information are classified as high risk, either because the exposure of this information can cause harm or because the information is specifically protected under law or contract.	The storage of sensitive information must meet the University's Security of Sensitive Information Policy.
2	Thefts of unattended valuables are common.	All employees and contractors who are issued University-owned endpoints are responsible for safeguarding both hardware and data by securing it at all times using a security cable or locking it in a secured cabinet or room.
3	Passwords are an important aspect of computer security. They are the front line of protection for user accounts.	Do not share your account IDs or passwords with others and do not tape them to your endpoint equipment. Use strong passwords (Alphanumeric, etc. greater than 6 characters)
4	Unauthorized software might pose a threat to your endpoint, data, or the University's network (e.g. music file sharing, gambling/gaming, pop-up window solicitations, etc.). Pirated software (copied illegally or installed without a license) will subject the University to penalties in the case of a software audit.	Do not install unauthorized or pirated software. Do not access / download data from unknown sources.
5	The University invests a significant amount each year to the endpoint replacement budget.	Demonstrate good judgment with the use of your endpoint (e.g. keep food and liquids away from endpoints).
6	Endpoints are repurposed over their lifecycle	Do not label or personalize the appearance of a University-owned endpoint (e.g. stickers, ink).
7	Endpoints need to be assessed for usability and reliability by Technology prior to redeployment to another user.	Departments will contact Technology to initiate the assessment process to ensure an endpoint is ready for the next employee. Technology will assist with migrating important data.
8	Web browsers and other applications may store personal information during use. A user who does not log out may inadvertently give access to their personal data (email, documents, etc.) to the next user.	When finished using an endpoint in a public space, logout.

Appendix

Appendix A: Endpoint Use Types

Worker : Workstation

Endpoints provided to benefits-eligible faculty and staff (i.e. assigned to a specific employee).

Worker : Shared

Endpoints deployed to a department office for a shared job role, or in a location for use by multiple individuals over the course of a day or week. At the end of each term, if the endpoint is no longer needed, it will be returned to Technology and repurposed. In most cases, a Virtual Client Device will be used.

Loaner

Endpoints loaned to Faculty, Staff, or Students by Technology for temporary use.

General Access

Endpoints in common areas such as the including labs, classrooms, library, lobbies, dining halls, and cafés.

Workstation
Endpoint installed in a room but not attached to an Instrument, Podium, or Lectern.

Podium
Endpoint installed in a Podium or Lectern and connected to a media controller to display on a monitor and projector or flat-panel TV.

Appliance

Endpoint dedicated for use with a single software, hardware instrument or service.

Conference
Endpoint dedicated for use in a conference room (e.g. Zoom Room controller).

Instrument
Endpoint dedicated for use with an instrument (e.g. IR Spectrometer, NMR, Scantron). The endpoint hardware configuration will be determined based on the instrument manufacturer's recommended specifications.

Signage
Endpoint installed with TV screen for the purpose of a digital signage display.

Appendix B: Preferred Vendors

Hardware Type	Preferred Vendor
Windows Desktops, Laptops and tablets	Zones
Mac (Apple) Desktops and Laptops	SHI
Apple tablets (iPads)	SHI B&H
Virtual Client Devices	Zones
Peripherals	Zones GovConnection Amazon B&H

Appendix C: Employee Eligibility

Employee Type
Full-time, benefits-eligible Faculty and Staff
Part-time, benefits-eligible Faculty and Staff working at least 20 hours per week
Contingent staff with specific computing needs to perform their job function

Appendix D: Standard Hardware Configurations

Refer to 4.6 for peripherals included in each configuration bundle.

Desktops

Virtual Client Device	Cost
Dell Wyse 3040	$

Windows Desktop	Cost
Dell Optiplex 70x0 Processor: Intel Core i5 ProSupport Plus: Next Business Day Onsite, 3 Years 16GB RAM (memory) 256GB SSD	$$

Mac Desktop	Cost
Mac Mini Processor: Apple M2, M3 or M4 (depending on model) AppleCare+ Protection Plan 16GB RAM (memory) 256GB SSD	$$

Laptops

Windows Laptop	Cost
Dell Latitude 74x0 Screen: 14.0” (1920 x 1080) Weight: 2.7lb (1.22kg)) Processor: Intel Core i5 ProSupport Plus: Next Business Day Onsite, 3 Years 16GB RAM (memory) 256GB SSD	$$$

Mac Laptop	Cost
MacBook Air Screen: 13.3” (1440 x 900) Weight: 2.7-2.8 pounds (1.24-1.35 kg) Processor: Apple M1, M2 or M3 (depending on model) AppleCare+ Protection Plan 16GB RAM (memory) 256GB Flash Storage	$$

Peripherals

Monitors

Unless a desktop has a built-in monitor, faculty & staff bundles will be configured with a Dell 24-inch QHD USB-C monitor. Monitors for other user cases may be substituted with a Dell 21.5-inch monitor with a resolution of at least 1920x1080 (Full HD). External monitors are optional with laptop bundles. In cases where a larger screen or higher resolution is required by job function, larger screens will be provided upon University Leadership Team member approval.

Printers

As of July 1, 2016—Local desktop printers will not be provided by Technology. Existing local printers will be assessed a charge of $100/year to cover maintenance costs. All employees are encouraged to use departmental multifunction devices (MFDs) for printing, copying, and scanning.

Input Devices

Input devices are used to provide data and control signals to the endpoint. Examples include keyboards, mice, and external webcams.

Laptop Docking Stations

Docking stations are no longer provided with laptop bundles. Instead a multiport video adapter is provided.

Video Adapters

Video adapters convert the video output interface (e.g. DisplayPort to VGA) and may be needed for external monitors and projectors. Laptops may need a video adapter to connect to a monitor provided in a configuration bundle. All laptop bundles will be deployed with a USB-C multiport adaptor. The adaptor will be configured with the following ports: 2 USB3, 1 HDMI, 1 Ethernet (RJ45), and 1 USB-C power delivery.

Appendix E: Standard Software Configurations

The following software will be installed on all University-owned endpoints running either Microsoft Windows or Apple macOS.

Windows	Version	Mac	Version
Operating System			
Microsoft Windows	10 (64-bit)	Apple macOS	15.x
Office / Productivity			
Adobe Creative Cloud App	latest	Adobe Creative Cloud App	latest
Adobe Reader	latest	Adobe Reader	latest
IBM SPSS	29		
Microsoft Office	2021	Microsoft Office	2021
Zoom	latest	Zoom	latest
Web Browsers			
Microsoft Edge	latest	Apple Safari	latest
Google Chrome	latest	Google Chrome	latest
Mozilla Firefox ESR	latest	Mozilla Firefox ESR	latest
Utilities			
Google Drive for Desktop	latest	Google Drive for Desktop	latest
Java Runtime Environment	latest	Java Runtime Environment	latest
7-zip	latest	Archive Utility	latest
Management / Security			
Alertus Desktop Client	latest	Alertus Desktop Client	latest
BigFix Agent	latest	BigFix Agent	latest
Check Point Mobile VPN Client	latest	Endpoint Security VPN	latest
Sassafras K2 Client	latest	Sassafras K2 Client	latest
Microsoft Defender	latest	Microsoft Defender	latest
Dell Command Update	latest		
Video / Graphics / Multimedia			
Panopto	latest	Panopto	latest

VLC	latest	VLC	latest
Virtualization			
VMware Horizon Client	latest	VMware Horizon Client	latest

Appendix F: Virtual Desktop Infrastructure (VDI)

Technology has deployed the virtual desktop infrastructure (VDI) solution VMware Horizon. Unlike traditional PCs, VMware Horizon desktops reside on servers located on-campus. This enables end-users to access virtual desktops using endpoints in any location with internet access. VDI client computers are deployed throughout the campus in common areas, labs, classrooms and some shared workstations.

Additionally, all managed endpoints have the VMware Horizon client installed. This client may also be downloaded for free by visiting https://apps.simmons.edu/. The client is also available for iOS devices through the Apple App Store and Android devices through Google Play.

To access the University's VDI, connect to **apps.simmons.edu** and enter your Simmons University username and password.

Appendix G: Mobile Devices

Mobile devices such as smartphones and tablets must be approved by a member of the University Leadership Team and are provisioned by Technology. Please see the University's Mobile Device policy for additional information.