Simmons College
Technology Endpoint Guidelines

Introduction

This document describes the guidelines used by Simmons Technology to manage the allocation and replacement of the 1,800+ desktop computers, laptop computers, thin clients, tablet devices, and mobile devices (collectively, "endpoint devices") that are owned by Simmons College. This includes endpoint devices that are used by individual faculty and staff, used in shared workspaces, in computer labs and classrooms, general-access kiosk computers, and devices loaned for temporary use.

Endpoint hardware is allocated to individual faculty and staff based on job function needs. These guidelines are in place to enable faculty and staff to perform their job duties, while also maximizing the useful life of each endpoint, and maximizing the efficiency of Simmons College's resources. The default endpoint is a Windows-based desktop or thin client device. Based on job requirements, a Windows laptop or Apple Mac desktop or laptop may be deployed.

Overview

Definitions

Endpoint: a [desktop](#) or [laptop](#) computer, [Thin or Zero Client](#), or [mobile device](#) running an operating system (Android, Chrome OS, iOS, OS X, Windows). Simmons Technology sets the replacement guidelines that define the level of deployment and support services for users throughout Simmons.

Peripheral: includes keyboards, mice, monitors, scanners, and printers.

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

- Simmons-issued 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 academic/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 Simmons 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

Guidelines

1. Lifecycle Management

1.1. Technology will order, receive, maintain, and dispose of or recycle all endpoints that are purchased by Simmons and are considered Simmons assets.

1.2. Support for all endpoints that are considered Simmons assets will be provided by the Technology Service Desk. All information about support services, including hours and contacts, will be provided at http://servicedesk.simmons.edu/.

1.3. Endpoints will be replaced on a cycle determined by the offices of the Chief Financial Officer and the Provost based on academic need, financial resources, and the College's strategic plans. At the end of each cycle, Technology will conduct a fleet assessment and recommend options for approval by Chief Financial Officer and the Provost. The faculty and staff replacement cycle is separate from the classroom, lab, and general access replacement cycle, which serves a different purpose.

1.4. 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.

1.5. 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.

1.6. 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.

1.7. 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.

1.8.   Simmons does not offer legacy endpoints for personal purchase. Employees may purchase equipment through vendor purchasing programs.

1.9.   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.

1.10.   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.

1.11.   Endpoints deployed off-campus (e.g. SLIS West, Online Faculty) will be configured with a local user account for access.

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

1.13.   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.

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

2.   Local Department Management

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

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 Simmons Technology Acceptable Use Policy and Information Security Policy.
2	Technology must know the location of endpoints to assist with hardware and software repairs.	Local Department and lab administrators will coordinate with Technology to move, replace, or

	Technology must report missing endpoints and their last known location to Public Safety.	locate hardware components. This includes the installation of aftermarket parts and components.
3	To prevent unscheduled downtime or a 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	Workstations must be joined to the Simmons 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 endpoints can be added to prevent any departmental impact.	All workstations must be joined to the Simmons 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 College'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 owned by Simmons and are considered Simmons 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 College's preferred vendors and verify they still meet academic needs, financial resources, and the College'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 Operating Team member and may not be managed by Technology.

3.7.   Simmons 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.   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 Operating Team member.

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

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

3.11.   When a department requires an enhanced bundle configuration for everyday operations, the appropriate Operating 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.

3.12.   Additional peripherals beyond the standard bundle (see 4.2) not included in a configuration bundle will be funded by the department of the requestor and acquired through Technology.

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

3.14.   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.

3.15.   Endpoints purchased for personal ownership using Simmons funds (e.g. development funds) are considered personal assets, not Simmons assets, and will not be managed by Technology.

3.16.   Endpoints deployed to off-campus employees (e.g. Online Faculty) will be shipped to and from campus using a preferred shipping vendor. Packing slips will be acquired through Technology.

4.   Hardware

4.1.   Technology will maintain a set of standard endpoint hardware configuration bundles, and assign endpoint bundles based on job function requirements. Configurations will be designed to be as versatile as possible to support all departments and job roles. Requests for laptops and other enhanced configurations, including endpoints running Mac OS X, must be approved by the appropriate Operating Team member.

§	Configuration Bundle	Justification	Cost	Approval
1	Virtual Desktop (VDI) Zero Client	Standard employee computer configuration.	$450	N/A
2	Standard Windows Desktop	Job function requires additional local storage, computing power, or graphics functionality.	$800	N/A
3	High Performance Windows Desktop	Job function requires significant storage, computing, or graphics performance. (For example: video editing, graphics processing.)	$1,000	Director
4	Standard Windows Laptop	Job function requires computing portability.	$1,200	Operating Team
5	High Performance Windows Laptop	Job function requires computing portability and high computing or graphics performance.	$1,500	Operating Team
6	Mac (Apple) Hardware	Job function has specific requirements available only using Apple products.	$1,300 - $1,500	Operating Team

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

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

§	Configuration Bundle	Peripherals
1	Desktop / Zero Client	One (1) Monitor (may be built-in) One (1) Keyboard One (1) Mouse
2	Laptop	One (1) Monitor One (1) Keyboard One (1) Mouse One (1) Laptop Docking Station One (1) Security Cable One (1) Video Adapter

4.3.   If an employee's department, job role, or employee type changes, any request for a new configuration bundle must be approved by the appropriate party.

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

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

4.5.   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 College.

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 Simmons 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 College 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 College'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 curriculum are needed. Technology needs time to not only build the package, but to test it with the appropriate liaison within the department or lab to ensure it meets their needs and performs in a stable manner.

5.7. New software requests – including upgrades – must meet the following guideline:

§	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 www.lynda.com

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

6.3. Reference sheets with tips, shortcuts, and how-to explanations for commonly used

features in the software.

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 College's Security of Sensitive Information Policy.
2	Thefts of unattended valuables occur on campus nearly everyday.	All employees and contractors who are issued Simmons 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. Utilize strong passwords (Alphanumeric, etc. greater than 6 characters)
4	Unauthorized software might pose a threat to your endpoint, data, or the Simmons network (e.g. music file sharing, gambling/gaming, pop-up window solicitations, etc.). Pirated software (copied illegally or installed without a license) will subject Simmons 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	Simmons 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 Simmons 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

Faculty / Staff Individual

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

Classroom / Lab / Event Space / Meeting Room

Endpoints deployed to rooms used for teaching, events, and meetings.

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. These endpoints are primarily used by instructors and lecturers.

Workstation

Endpoint installed in a room but not attached to an Instrument, Podium, or Lectern. These endpoints are primary used by students.

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.

Department 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 Desktop (VDI) Zero Client will be used in this case.

General Access

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

Kiosk

Endpoint designed for internet access, and does not require a user to log in and may be used by anyone with physical access.

Workstation

Endpoint requires a user to log in and may be used by anyone with a Simmons username and password.

Loaner

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

Appendix B: Preferred Vendors

Vendor	Hardware Type
Zones	Windows Desktops and Laptops
Apple eCommerce	Mac (Apple) Desktops and Laptops
Zones, GovConnection	Peripherals

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

Appendix D: Standard Hardware Configuration Bundles

Desktops

Virtual Desktop	Cost
Dell Wyse P25 Dell wired keyboard and mouse	$

Standard Windows Desktop	Cost
Dell Optiplex 3040 Intel Core i5 processor 8GB RAM (memory) - expandable 256GB SSD or higher Dell wired keyboard and mouse	$$

High Performance Windows Desktop	Cost
Dell Optiplex 7040 Intel Core i7 processor 16GB RAM (memory) 256GB SSD or higher Dell wired keyboard and mouse	$$$

Standard Mac Desktop	Cost
21.5-inch iMac Intel Core i5 processor 16GB RAM (memory) 256GB SSD or higher Apple wired keyboard and mouse	$$$

High Performance Mac Desktop	Cost
21.5-inch iMac Intel Core i7 processor 16GB RAM (memory) 256GB SSD or higher Apple wired keyboard and mouse	$$$$

Laptops

Standard Windows Laptop	Cost

Dell Latitude E7470 Screen: 14.0" (1920 x 1080) Weight: 3.43lbs (1.56kg) Processor: Intel Core i5 8GB RAM (memory) 256GB SSD or higher Dell wired keyboard and mouse	$$$

High Performance Windows Laptop	Cost
Dell Latitude E7470 Screen: 14.0" (1920 x 1080) Weight: 3.43lbs (1.56kg) Processor: Intel Core i7 16GB RAM (memory) 256GB SSD or higher Dell wired keyboard and mouse	$$$$

Standard Mac Laptop	Cost
MacBook Air Screen: 13.3" (1440 x 900) Weight: 2.96 pounds (1.35 kg) Processor: Intel Core i5 AppleCare Protection Plan 8GB RAM (memory) 256GB Flash Storage Apple wired keyboard and Logitech mouse	$$$

High Performance Mac Laptop	Cost
MacBook Pro with Retina display Screen: 13.3" (1680 x 1050 scaled) Weight: 3.48 pounds (1.58 kg) Processor: Intel Core i7 AppleCare Protection Plan 16GB RAM (memory) 256GB Flash Storage Apple wired keyboard and Logitech mouse	$$$$

Peripherals

Monitors

Most desktop and laptop bundles will be configured with a Dell 21.5-inch monitor with a resolution of 1920x1080. In cases where a larger screen or higher resolution is required by job function, larger screens will be provided upon Operating 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 multi-function 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 provide a simplified way of plugging laptops into common peripherals through port replication.

Video Adapters

Video adapters convert the 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.

Because manufacturers change their product line-up periodically (e.g. internal processor/chip or video card), Technology will negotiate new standard configurations in order to maintain consistency, performance, price, and suitability for Simmons business. Technology will document changes as they occur.

Appendix E: Standard Software Configurations

The following software will be installed on all Simmons Desktop and Laptop Endpoints running either Microsoft Windows or Mac (Apple) OS X.

Windows	Version	Mac (Apple)	Version
OS		**OS**	
Microsoft Windows	10 (64-bit)	OS X	10.11.x
Office / Productivity		**Office / Productivity**	

Adobe Reader	latest	Adobe Reader	latest
Citrix GoToMeeting	latest	Citrix GoToMeeting	latest
Skype	latest	Skype	latest
Microsoft Office	2016	Microsoft Office	2016
File transfer		**File transfer**	
WinSCP	latest	Cyberduck	latest
Web Browsers		**Web Browsers**	
Internet Explorer / Edge	latest	Apple Safari	latest
Mozilla Firefox	latest	Mozilla Firefox	latest
Google Chrome	latest	Google Chrome	latest
Utilities		**Utilities**	
Java	latest	Java	latest
7-zip	latest	Stuffit Expander	latest
Software License Management		**Software License Management**	
BigFix Agent	latest	BigFix Agent	latest
K2 Client	latest	K2 Client	latest
Video / Graphics / Multimedia		**Video / Graphics / Multimedia**	
Adobe Flash	latest	Adobe Flash	latest
Adobe Shockwave	latest	Adobe Shockwave	latest
Apple Quicktime	latest	Apple Quicktime	latest
Microsoft Silverlight	latest	Microsoft Silverlight	latest
VLC	latest	VLC	latest
Security		**Security**	
ESET Endpoint Antivirus	latest	ESET Endpoint Antivirus	latest
Virtualization		**Virtualization**	
VMware Horizon Client	latest	VMware Horizon Client	latest

VPN		VPN	
Check Point Mobile VPN Client	latest	Check Point Mobile VPN Client	latest

Appendix F: Virtual Desktop Infrastructure (VDI)

Simmons Technology is deploying the virtual desktop infrastructure (VDI) solution VMware Horizon View. Unlike traditional PCs, VMware Horizon View desktops reside in the cloud on Simmons servers located on-campus. This enables end users to access virtual desktops using Windows- or Mac-based laptops or desktops, thin clients, zero clients, or mobile devices from home, office, and anywhere with Internet access.

Where appropriate, Simmons faculty and staff who normally use a desktop computer configuration will be equipped with a Virtual Desktop terminal. These devices are more cost-effective, and have a longer useful life than traditional desktop computers.

Additionally, all Simmons-owned computers have the VMware Horizon View 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 connect to the Simmons VMware Horizon View instance, connect to **apps.simmons.edu** and enter your Simmons username and password. Select the Virtual Desktop you want to access.

Appendix G: Mobile Devices

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