109: IT Hardware Lifecycle

100: Office Administration · https://milo.masseyservices.com/docs/109-it-hardware-lifecycle/

Section: Office Administration
Subject: IT Hardware Lifecycle
Approved by: Tony Massey
Effective Date: 21 November 2023
Last Reviewed Date: 21 November 2023
Policy Owner: Vice President of Information Technology

Policy

Our current licensing model ties each user to a single workstation, which includes an operating system, a productivity suite (Microsoft Office), and security and management software. An analysis of equipment in active use shows an increase in “spare” workstations and equipment that has neither been reassigned nor recovered by IT for disposal and have not been properly licensed.

To maintain a rigorous security posture, the IT department will begin raising the requirements for spare workstation equipment.

Workstations (i.e., laptops and desktop PCs)

When a change event occurs (i.e., a new workstation purchase, a team member term, etc.), the previous equipment will be surrendered at the time of deployment. IT will then re-image the equipment. From there, it can either be re-deployed to someone else in the same department (who will, in turn, surrender their previous device), or, if eligible, entered into the loaner pool, which is used by all departments. If it’s not eligible for the loaner pool, it will be wiped and recycled.

If a department head chooses to reassign a laptop to another team member in their department, either as a backup or for redeployment, it must be authorized by a Vice President, and a CER will need to be completed to keep the device fully licensed. These licenses include an operating system (e.g., Windows, macOS), management software (e.g., KACE, Moysle, etc.), all security software (e.g.,

Crowdstrike), and, if necessary, the Office suite. The device will need to be stored in a powered-on state and connected to our network in order to receive updates. Any device that is not connected to our network will be administratively deactivated and placed into a locked mode, to the extent IT can reach it.

Printers, Copiers, and Multifunction Devices

When a printer is replaced, it will be removed from our network. Only printers and MFDs on the approved list, which is maintained by IT, will be network connected.

Tablets and iPads

All tablets and iPads must run our Mobile Device Management (MDM) software (currently JAMF) and kept up to date. Personal devices must meet minimum security standards to use Massey-related services.

Mobile Phones

Massey-owned mobile phones must run our Mobile Device Management (MDM) software (currently JAMF) and kept up to date. Personal devices must meet minimum security standards to use Massey-related services.

Peripherals

Workstation peripherals should be purchased through IT. IT will not reimburse you for monitors, mice, keyboards, storage devices, stands, chargers, tablet accessories, or any other peripherals. Peripherals not approved by IT or compatible with existing hardware standards will not be supported.

Third Party Devices

Non-standard devices, such as macOS or Linux laptops, “smart” devices, appliances, IoT devices, etc., including TVs and smart assistants, will not be used on the Massey network without prior authorization from IT.

No third-party devices, including personal devices, will be connected to our Corporate non-personal, non-guest network.

IT will not support devices that have been brought in from home. No workstation/laptop/desktop, console, tablet, or phone that is not Massey-owned or approved by Massey IT will be supported. If a device has been approved by Massey IT, it will require appropriate licensing and must run the recommended MDM and/or endpoint protection software.

Because of the potential security risks of these devices introduce, any device on the Massey network without authorization will result in a disciplinary action report.

Downloads

Embedded media: https://milo.masseyservices.com/wp-content/uploads/2025/09/109-IT-Hardware-Lifecycle.pdf

109 IT Hardware LifecycleDownload