UNIVERSITY of WISCONSIN
UWMILWAUKEE

Standard for UW-Milwaukee Apple Macintosh Computers

Summary

This document defines and describes the standard expected for all University of Wisconsin-Milwaukee owned Macintosh devices.

The underlying standard for all UWM-owned devices is full compliance with UW-System & UW-Milwaukee policies and practices[i]. The steps outlined here function as a guide to ensure that UWM's Apple Macintosh devices meet this standard and maintain the security and integrity of UW data accessed, generated, and stored on these devices.

This standard streamlines the provisioning, deployment, and support of the devices throughout their lifecycle. Devices that fail to comply with these standards may be ineligible for support from Campus Technology Support and University IT Services and may be excluded from campus services such as file storage, printing, and network access.

1. All campus Macs must be enrolled in Apple's deployment services (DEP).
2. All campus Macs must be enrolled in UWM's official Mobile Device Management (MDM) solution.
3. All campus Macs for faculty, staff, or student use will authenticate using a cloud-hosted identity provider (IdP).
4. All campus Macs must run a supported version of the Macintosh operating system, macOS.

Campus Mac Standard in Detail

1. **All campus Macs must be enrolled in Apple's deployment services (DEP).**

   Apple provides deployment services through Apple School Manager via their Device Enrollment Program (DEP) which is critical to device provisioning and management. Having a device enrolled in Apple School Manager does not necessarily mean that the device is managed but is necessary for automating the management process.

   Device serial numbers enrolled in Apple School Manager are tied to UWM. During the device setup process, MDM configuration information is automatically pushed to the device even if it had previously been removed from management, had its boot volume replaced, and/or is no longer connected to a UWM network.

2. **All campus Macs must be enrolled in UWM's official Mobile Device Management (MDM) solution.**

   Mobile Device Management is handled by Jamf Pro and is where devices come into management after being activated through DEP. It is in this phase that CIS device hardening standards, UW-System Policy, and UWM practices are applied. These settings are applied to provide adequate protection for all campus data accessed, created, or manipulated on these devices.

Devices whose primary function requires non-compliance with UW-System Policy (e.g., a computer used to research the effects of malicious software) are still required to be in management; however, they can have the applied policies limited to meet the needs of the use case. Before a device can be excluded from any management policy, a business use case for the exception must be documented and approved by the UWM Information Security Office. These exceptions will require compensating controls be applied to ensure system integrity. See the section on noncompliance at the end of this document for further information.

3. **All campus Macs for faculty, staff, or student use will authenticate using a cloud-hosted identity provider (IdP).**

   Microsoft Azure Active Directory (AD) is currently the approved cloud-hosted identity provider for UW-Milwaukee and Jamf Connect is used to authenticate users and sync local account information with directory services. This enables users to securely authenticate to their devices and services without the need to be physically located on campus or be connected to campus via VPN.

   Azure AD services are used to enforce minimum requirements for password and passphrase complexity and expiration, account lockout policies and other UW System authentication requirements.

   The use of Jamf Connect with Azure AD allows for full compliance with authentication policies, follows best-practice recommendations from Apple, and provides the best possible user experience for any computer not directly connected to the UWM network.

4. **All campus Macs must run a supported version of the Macintosh operating system, macOS.**

   New versions of the Macintosh computer operating system, macOS, typically include new security features in addition to patches for vulnerabilities, therefore every effort is made to ensure devices in the fleet are running the latest version of macOS wherever possible.

   Apple releases new versions of macOS annually in the Fall and releases are supported with feature updates for one year and security updates for three years. Apple typically discontinues all macOS and hardware support for devices after seven years. This leaves devices capable of running an OS that is patched with security updates from Apple up to nine years after it was released.

   Example of macOS release support from Fall 2020:

   > **macOS 11.01 –** Released in Fall 2020, **feature and security updates** from Apple, highest supported release for 2013 devices.
   >
   > **macOS 10.15 –** Released in fall 2019, **security updates** from Apple, highest supported release for 2012 devices.
   >
   > **macOS 10.14 –** Released in fall 2018, **security updates** from Apple, highest supported release for 2011 devices.

macOS 10.13 – Released in fall 2017, **unsupported**, highest supported release for 2010 devices.

To ensure that Apple devices remain secure, the device's primary OS should not fall out of support. If research requirements or other extenuating circumstances dictate the need for unsupported versions of macOS, they should be compartmentalized in virtual machines or removed from the network where possible. Devices that cannot run a supported version of macOS should be replaced.

Please refer to the CTS Support Practice for Managed Apple Devices for more information.

Noncompliance

Devices needing to operate outside of this standard will need:

- A documented business need for noncompliance.
- Compensating controls applied to ensure that the goals of the original policy are met.
- Approval by the UWM Information Security Office that the business need is valid and that the compensating controls are adequate.

Approvals for noncompliance are subject to period review. Failure to comply with information technology resource policies are addressed in *UW System Regent Policy Document 25-3: Acceptable Use of Information Technology Resources.*

Changelog

04/29/2021 – Submitted to Information Security Office and Chief Information Officer for adoption.

[i] UW-System policies and practices met by this standard include:

UW System Administrative Policy 1030: Information Security: Authentication

UW System Administrative Policy 1031: Information Security: Data Classification and Protection

UW System Administrative Policy 1035: Information Security: IT Asset Management

UW System Administrative Policy 1039: Information Security: Risk Management

All management settings, policies, and procedures are designed to adhere to UW System Administrative Policy 1040: Information Security: Privacy Policy