IT Standard on End User Device Supportability

Revision Notes: Version 1.0	Ratified: 5/24/22	Status: APPROVED

Table of Contents

1. Objective

1.1. This standard defines 1) University owned end user device minimum criteria for supportability, 2) managed end user device requirements, and 3) responsibilities for onboarding and offboarding end user devices for the effective and efficient management of end user devices to support University operations and readiness needs, and meet the Minimum Security Standard throughout the end user device lifecycle at an affordable cost.

2. Scope

2.1. This standard applies to all University owned end user devices which are defined in this IT standard as a laptop or desktop computer, or Apple Mobile Device and to all University employees.

3. End User Device Minimum Criteria

3.1. End user devices with Windows Operating System and Apple Operating System: end user devices must have either the last released major Windows or Apple Operating system or the version one behind the last released Windows OS, macOS, iOS, iPadOS, or tvOS and need to be able to meet Managed end user device Requirements (section 4).

3.2. End user devices with Chrome Operating System: end user devices must be enrolled in a device management system.

3.3. For end user devices already in circulation, there will be a 6 month grace period, starting from the date when ITS begins deploying and/or discontinues blocking the latest Operating System on managed devices, in order for users to upgrade or replace devices that do not meet the End User Device Supportability Standard.

4. Managed End User Device Requirements

4.1. To effectively manage end user devices and meet the Minimum Security Standard Requirements to protect institutional data, University end user devices will be managed by a device management system through Information Technology Services.

4.2. ITS Infrastructure and Systems will enforce settings and policies to protect institutional data and ensure supportability on managed end user devices.

5. End User Device Onboarding and Offboarding Procedures

5.1. ITS Support will maintain end user device Onboarding procedures to ensure that all end user devices are 1) enrolled in the approved device management system, 2) have the required software, settings, and policies for managed end user devices prior to usage by the assigned user, and 3) are updated in the appropriate end user device inventory system.

5.2. ITS Support will maintain end user device Offboarding procedures to ensure that end user devices are: 1) reclaimed when an employee leaves their position at the University or is assigned a replacement end user device, 2) are cleaned of any University data and re-purposed when possible, 3) removed from appropriate device management systems at end of life and 4) the appropriate end user device inventory system is updated.

5.2.1. When an end user device no longer meets this standard, IT Support will notify the end user that they have 6 months to replace the device before the device will be excluded from the campus network and campus resources (e.g., VPN).

5.3. ITS Support will review any significant changes to the end user device Onboarding and Offboarding procedures with the Client Management Governance Group for advisement.

5.4. The Chief Information Officer, or delegate, will approve all changes to end user device Onboarding and Offboarding Procedures.

6. End User Responsibilities

6.1. To ensure that On Boarding procedures are performed, end users are responsible for contacting their IT support unit when acquiring a new end user device if the acquisition does not originate with the IT support unit.

6.2. To ensure that Off Boarding procedures are performed, end users are responsible for contacting IT Support when either discontinuing use of an end user device (for replacement or retirement) or transferring an end user device to another employee.

6.3. To ensure that managed device requirements are met, end users are responsible for:

6.3.1. Follow user-initiated upgrade installation procedures in order to install a supported Operating System, and/or

6.3.2. If the hardware no longer meets the End User Device Supportability Standard, contact IT Support for remediation.

7. Enforcement, Exemptions, and Advisement

7.1. **Authority and Enforceability -** This standard is established under the authority of the Chief Information Officer.

7.2. **Exemptions -** Exemptions must receive approval by the Chief Information Officer or delegate.

7.3. **Review and Advisement -** The Client Management Governance Group will review the minimum end user device criteria and managed end user device criteria on an annual basis, at minimum. IT Governance and pertinent Technical Advisory Groups provide collaborative advisement concerning standards.

8. Definitions

8.1. End User Device: any laptop, desktop, mobile device, or computing instrument used to support or conduct official University business. Also referred to as an endpoint

8.2. Managed end user device: end user devices that are enrolled in an Appalachian State University device management system

8.3. Device management system: an IT system to 1) proactively manage security risks and vulnerability, 2) receive automatic operating system updates and needed software, and 3) provide a consistent employee device experience.

9. References and Related Policies and Standards

9.1. Minimum Security Standard

9.2. University Infrastructure and Architecture Policy

9.3. University Information Security Policy

9.4. University Information Technology Governance Policy

10. Contacts for Questions or Information About this Standard

Office contact	Phone	Online/Email
Chief Information Officer	828-262-6278	cio@appstate.edu