CALIFORNIA STATE UNIVERSITY
FULLERTON

Endpoint System Baseline

Division:
Information Technology

Contact Information:
Information Security Office

Revision History:

Version No	Date	Description	Author
1	2/18/2026	Initial Release	Jay Lin

Purpose:

Endpoints (such as laptops, desktops, and mobile device) are critical resources for the Division of Information Technology.
The purpose of this Endpoint System Security Baseline is to define the minimum security configuration requirements for endpoint devices connected to the university network.
This baseline helps ensure that endpoint systems are configured securely to reduce cybersecurity risks, protect institutional data, and support the university's information security policies.

Scope:

This baseline applies to all university-owned or managed endpoint systems, including but not limited to:

- Desktop Computer: Windows, Mac, Linux
- Laptop Computer: Windows, Mac, Linux
- Mobile Devices: Apple and Andorid

Baseline Requirement:

- All endpoints must be inventoried and tracked by the IT Asset Management team.
- All endpoints must run a vendor-supported operating system.
    - Windows and macOS systems must run supported versions receiving active security updates.
    - Linux must use a vendor-supported distribution that receives active security updates.

- End-of-Support operating systems are not permitted.

- All Windows endpoints must be joined to the campus Active Directory Domain Services (AD DS).
- Remote-provisioned Windows endpoints must be enrolled in the campus Microsoft Intune tenant.
- All macOS endpoints must be enrolled in the campus Mobile Device Management (MDM) platform (Jamf).
- Linux systems should be joined to Active Directory or an approved centralized identity management system, where technically feasible.
- All endpoints connected to the campus network must be protected using an approved Endpoint Protection Platform (EPP).
    - Anti-Malware
        - Windows Defender
        - MAC Defender
        - Linux Defender
    - Personal Firewalls
        - Personal firewalls must be enabled on the endpoint for security protection

- Endpoints must use encrypted communication protocols when transmitting university data in accordance with the Data Classification Standard.
  Examples include:
    - HTTPS
    - SSH
    - SFTP
    - TLS-based services
- Endpoint devices that do not require wireless connectivity should have wireless capability disabled when feasible.
- Endpoint authentication must follow the Information Security Office Password Procedures.
- Mobile endpoints must be enrolled in the campus Mobile Device Management (MDM) system.
- All endpoints must follow the campus patch management process, including automated patch deployment using SCCM, Intune, Jamf, or other approved tools.
- Endpoint systems that store university data must perform regular data backups using approved backup services such as Dropbox.
- Endpoint systems must enforce the principle of least privilege, ensuring users only receive access necessary to perform their job responsibilities.
- Remote access to campus systems must use the campus standard VPN solution (GlobalProtect) when accessing university resources from external networks.