

Endpoint Protection Standard

Owner	Andrew Smith, Security Owner
Version	1.1, effective October 19, 2026
Part of	Swapt Information Security Policy

1. Scope and coverage

This standard applies to every laptop or desktop used to access Swapt systems, source code or data ("endpoints"). Swapt personnel work on company Apple Mac computers running a supported version of macOS. Coverage is 100% of these endpoints. A device that doesn't meet this standard may not be used to access Swapt systems.

2. Anti-malware protection

Every endpoint runs Apple's built-in, always-on malware protection, which cannot be turned off by ordinary use:

- **XProtect** scans applications and files for known malware when they are opened or changed. Its signatures update automatically and independently of macOS updates.
- **XProtect Remediator** scans in the background on a regular schedule and removes known malware it finds.
- **Gatekeeper and notarization** block software that isn't signed by an identified developer and checked by Apple, unless a user explicitly overrides it.
- **System Integrity Protection** stops malicious software from changing protected system files.

Gatekeeper and System Integrity Protection must stay enabled. Users must not override malware warnings.

3. Updates

- Automatic macOS updates are enabled, including "Install Security Responses and system files", so XProtect signatures and Rapid Security Responses install automatically.
- Critical macOS security updates are installed within 7 days of release, and other security updates within 30 days.
- Browsers and development tools are kept on supported versions with auto-update turned on.

4. Device hardening

- FileVault full-disk encryption is enabled on every endpoint.

- The macOS firewall is enabled.
- Screen lock settings follow the Security Baseline Standard.
- Software is installed only from the Mac App Store, identified developers or official package managers.

5. Verification

- When a device is first given to someone, the Security Owner checks that FileVault, Gatekeeper, System Integrity Protection, the firewall and automatic updates are turned on.
- Every quarter, each person confirms these settings on their device, and the Security Owner records the result in the security log.
- Any device that falls short is fixed before it is used again for Swapt work.

6. Lost or stolen devices

A lost or stolen device must be reported to the Security Owner immediately. The device is remotely locked or wiped through Find My, the user's account sessions and tokens are revoked, and the event is handled under the Incident Response Plan.