Synthetic Users Endpoint Security & Device Management Policy

Version: 1.0

Effective Date: 15 February 2026

Owner: Security & Compliance Lead

Approved by: CTO

---

1. Purpose

This policy defines the security requirements for all endpoint devices used by Synthetic Users employees to access corporate and production systems.

---

2. Scope

This policy applies to all employee workstations and devices that access Synthetic Users systems or data. The current fleet consists exclusively of Apple MacBooks.

---

3. Device Standards

3.1 Approved Devices

- Only company-issued or company-approved Apple MacBooks are authorized for work use.
- Personal devices may not be used to access corporate or production systems.

3.2 Full Disk Encryption

- All devices must have **FileVault** (macOS full disk encryption) enabled.
- Encryption status is verified through SOC 2 compliance monitoring tooling.
- Devices found without encryption enabled will be flagged for immediate remediation.

3.3 Anti-Malware Protection

- All devices rely on **macOS built-in security protections**, including:
  - **XProtect** — Signature-based malware detection, automatically updated by Apple.
  - **Gatekeeper** — Ensures only trusted software from identified developers or the App Store can run.
  - **MRT (Malware Removal Tool)** — Automatically removes known malware.
- Anti-malware status is monitored through Sprinto (Dr. Sprinto MDM).

3.4 Operating System Updates

- macOS updates are installed automatically shortly after release.
- Critical security patches must be applied within 72 hours of availability.

3.5 Screen Lock

- Devices must be configured to lock automatically after a maximum of 5 minutes of inactivity.
- Employees must manually lock devices when stepping away.

---

4. Device Monitoring & Compliance

- All devices are registered and monitored centrally through Sprinto.
- Compliance checks include:
  - FileVault encryption enabled
  - macOS version up to date
  - Screen lock configured

    - Anti-malware protections active
- Non-compliant devices are flagged and must be remediated within 48 hours.

5. Removable Media

- Employees do not have access to corporate customer data on their local devices that could be exfiltrated via removable media.
- All customer data resides in cloud-hosted systems accessed through authenticated web interfaces.
- USB storage device controls are not enforced via MDM, as the data architecture eliminates the local data exfiltration risk.

6. Mobile Devices

- Corporate email and systems are accessed via Google Workspace on mobile devices.
- Google Workspace mobile management policies enforce screen lock and remote wipe capability.
- No customer data is accessible from mobile devices.

7. Lost or Stolen Devices

- Employees must report lost or stolen devices to the security team immediately.
- The security team will revoke device access and initiate remote wipe if applicable.
- SSO sessions for the affected user will be revoked.

8. Review

This policy is reviewed annually or when changes to the device fleet or security tooling occur.