FIPS 140-2 Endpoint Compliance Checklist

Practical, auditor-friendly steps to deploy and verify FIPS-aligned crypto on managed endpoints using Codeproof.

Note: FIPS validation applies to cryptographic modules (OS libraries, HSMs). Codeproof enforces device/app policies and helps you gather evidence; your organization selects FIPS-validated modules and remains responsible for overall compliance. FIPS 140-3 supersedes 140-2—confirm your authority's timelines.

1) Scope & Applicability

- Define systems that process, store, or transmit sensitive data requiring FIPS 140-2 validated crypto.
- Identify platforms (Windows, macOS, iOS/iPadOS, Android, ChromeOS) and application crypto dependencies.
- Document versions/builds mapped to NIST CMVP certificates where applicable.

2) Asset Inventory & Ownership

- Maintain device, OS, and app inventory (owner, location, role, serial/UDID/IMEI).
- Tag systems that must operate in FIPS-required mode (e.g., federal/state contracts).
- Record crypto module IDs and certificate numbers when applicable.

3) Platform Baselines (configure via Codeproof)

- Enforce device encryption (BitLocker/FileVault/OS-native); escrow/recover keys per policy.
- Require strong passcode/biometric, auto-lock, and idle timeout; disable insecure unlock methods.
- Force OS updates and minimum OS versions; block jailbroken/rooted devices.
- Push trusted roots/intermediates and client certificates; rotate credentials periodically.
- Require TLS for all managed connections; block legacy protocols and weak ciphers where possible.

4) FIPS-Specific Controls & Verification

- Map each OS/app crypto dependency to a FIPS 140-2 validated module (CMVP) or an approved 140-3 successor.
- Windows: If required by your authority, enable 'System cryptography: Use FIPS compliant algorithms' policy; verify application compatibility.
- macOS/iOS/iPadOS: Verify use of platform cryptographic services; document Apple platform validation references where applicable.
- Android: Prefer devices/ROMs and apps that rely on platform crypto backed by validated modules; document OEM/SoC claims where relevant.
- VPN/Wi-Fi/Email: Enforce suites using approved algorithms (e.g., AES-GCM, SHA-2, ECDHE) and disable deprecated suites.

- Self-tests & module integrity: Record vendor documentation and validation certificate numbers for audited components.

5) Application Governance

- Allowlist required apps known to use approved crypto; block risky or unknown apps.
- Use managed configurations (per-app VPN, Open-In restrictions, clipboard controls) to contain data.
- For BYOD, use Android Work Profile / Apple User Enrollment; enable selective wipe.

6) Evidence for Auditors

Control	Codeproof Capability	Evidence to Export
Device encryption policy	Enforce BitLocker/FileVault; compliance rules	Device list with encryption status; policy snapshots
TLS/cipher enforcement	Push Wi-Fi/VPN profiles; cert distribution	Profile payloads; certificate inventory; connection logs (where available)
App allow/block	App catalogs, allowlists/denylists	App inventory/report; policy history
OS integrity/posture	Root/jailbreak detection; minimum OS	Compliance report; noncompliance actions
BYOD separation	Work Profile / User Enrollment; selective wipe	Wipe events; device assignment records
Key/cert lifecycle	Cert install/rotation; trusted roots	CA/PKI logs; MDM certificate push records

7) Change Control & Exceptions

- Record deviations and compensating controls for modules not yet validated; track remediation dates.
- Version-lock and test critical crypto-dependent apps before OS upgrades.
- Review policy baselines quarterly; re-validate module versions after major updates.