



# NIST SP 800-53 Endpoint Compliance Checklist

Practical checklist for aligning organizational endpoints with NIST SP 800-53 security and privacy controls using Codeproof UEM.

*Note: NIST SP 800-53 compliance requires a complete security and risk management framework. Codeproof provides device and application safeguards that support endpoint-level implementation of relevant NIST controls.*

## 1) Access Control (AC)

- Require unique IDs and strong authentication for all endpoint users.
- Configure auto-lock, idle timeout, and least privilege access.
- Support MFA for remote and privileged access.

## 2) Audit and Accountability (AU)

- Enable device-level logging of access, configuration, and policy changes.
- Retain logs consistent with organizational retention requirements.
- Export audit-ready reports of compliance status and endpoint posture.

## 3) System and Communications Protection (SC)

- Enforce device encryption for data at rest (BitLocker, FileVault, mobile encryption).
- Encrypt data in transit with TLS and IPsec VPN.
- Restrict unauthorized or legacy communication protocols.

## 4) Configuration Management (CM)

- Apply standardized baselines across Windows, macOS, iOS, and Android.
- Block installation of unauthorized or risky applications.
- Detect and block rooted or jailbroken devices.

## 5) System and Information Integrity (SI)

- Monitor OS and application versions for patching requirements.
- Quarantine or restrict access for unpatched or non-compliant devices.
- Enable malware and threat detection posture integration.

## 6) Incident Response (IR)

- Enable remote lock, Lost Mode, and full or selective wipe.
- Revoke credentials, certificates, and keys when incidents occur.
- Log all incident response actions for evidence and reporting.

## 7) Identification and Authentication (IA)

- Require device passcodes, biometrics, and MFA for sensitive apps.
- Distribute and manage digital certificates for authentication.

## 8) Security Assessment & Authorization (CA)

- Export compliance reports and device inventory for assessments.
- Document endpoint safeguards and enforcement history for auditors.

