ISO/IEC 27001 Endpoint Compliance Checklist

Practical checklist for aligning organizational endpoints with ISO/IEC 27001 information security controls using Codeproof UEM.

Note: ISO/IEC 27001 certification requires a full ISMS (Information Security Management System) with policies, risk assessments, and audits. Codeproof provides endpoint and application safeguards that support ISO 27001 Annex A controls.

1) Access Control (Annex A.9)

- Enforce unique user IDs and strong authentication on all endpoints.
- Apply least privilege by restricting access to sensitive applications and data.
- Configure auto-lock and idle timeout to prevent unauthorized access.

2) Cryptography (Annex A.10)

- Require device encryption across Windows, macOS, iOS, and Android devices.
- Ensure use of approved cryptographic algorithms for data at rest and in transit.
- Distribute and manage certificates securely via MDM.

3) Operations Security (Annex A.12)

- Deploy security baselines across devices, enforce updates and patch levels.
- Restrict installation of unauthorized applications.
- Detect and block rooted or jailbroken devices.

4) Communications Security (Annex A.13)

- Enforce secure Wi-Fi and VPN configurations with TLS/IPSec.
- Require per-app VPN for sensitive services.
- Block legacy or insecure communication protocols.

5) System Acquisition, Development and Maintenance (Annex A.14)

- Allow only approved applications and block unverified app stores.
- Apply managed configurations for apps to protect data flow and integrity.

6) Supplier Relationships (Annex A.15)

- Enforce controls for contractor or third-party managed devices.
- Use selective wipe on BYOD when offboarding or contracts end.

7) Information Security Incident Management (Annex A.16)

- Enable remote lock, Lost Mode, or selective/full wipe in case of compromise.
- Revoke keys, certificates, and credentials immediately when needed.
- Maintain incident records with device and user activity logs.

8) Compliance & Audit Evidence (Annex A.18)

- Maintain complete device inventory and security posture reports.
- Export historical configuration and compliance logs for auditors.
- Document encryption status, patch posture, and remote actions as evidence.

Copyright © Codeproof Technologies Inc. — This checklist supports ISO/IEC 27001 alignment on endpoints using Codeproof controls. It is not legal advice.