Muster-Prüfprogramm

Endgeräte- und Mobilgerätesicherheit

12 Prüfschritte · BSI, ISO 27001

12 Prüfschritte mit Kriterium, Fundstelle, Prüfhandlung und erwarteten Nachweisen. 8 Unterlagen zur Anforderung und die typischen Feststellungen.

ISO/IEC 27001:2022 Anhang A 8.1 · BSI SYS.2.1 · BSI SYS.3.2.2 · ISO/IEC 27001:2022 Anhang A 8.9 · ISO/IEC 27001:2022 Anhang A 8.7 · BSI OPS.1.1.4 · ISO/IEC 27001:2022 Anhang A 8.8 · BSI SYS.3.1 · ISO/IEC 27001:2022 Anhang A 8.24 · BSI SYS.3.2.1 · ISO/IEC 27001:2022 Anhang A 8.2 und 8.19 · ISO/IEC 27001:2022 Anhang A 7.10 · BSI SYS.4.5 · ISO/IEC 27001:2022 Anhang A 6.8 · ISO/IEC 27001:2022 Anhang A 5.11 und 7.14

Prüfungsziel und Geltungsbereich

Die Prüfung beurteilt, ob die Organisation ihre Endgeräte über den gesamten Lebenszyklus steuert: von der Inbetriebnahme mit einer gehärteten Standardkonfiguration über Schadprogrammschutz, Aktualisierung und Verschlüsselung bis zur Rückgabe und Löschung. Für mobile Geräte beurteilt sie, ob ein Mobile Device Management die Vorgaben wirksam durchsetzt.

GELTUNGSBEREICH

- Arbeitsplatzrechner und Laptops unter den eingesetzten Betriebssystemen
- Dienstliche Smartphones und Tablets sowie private Geräte, soweit sie dienstlich genutzt werden
- Werkzeuge für Softwareverteilung, Schadprogrammschutz und Mobile Device Management
- Nicht Gegenstand: Server und Netzkomponenten, die eigene Prüfprogramme haben

Prüfschritte 1 bis 3

Schritt 01 — ISO/IEC 27001:2022 Anhang A 8.1; BSI SYS.2.1

Eine Richtlinie regelt Beschaffung, Konfiguration, Nutzung und Rückgabe von Endgeräten einschließlich mobiler Geräte.

Prüfhandlung Richtlinie lesen, Freigabe prüfen und mit den tatsächlich eingesetzten Gerätetypen abgleichen.

Nachweise Endgeräterichtlinie mit Freigabe, Übersicht der Gerätetypen

Schritt 02 — ISO/IEC 27001:2022 Anhang A 8.1; BSI SYS.3.2.2

Nur verwaltete und registrierte Geräte erhalten Zugriff auf Unternehmensdaten.

Prüfhandlung Zugriffsregeln für E-Mail und Dateiablage ansehen und nachvollziehen, ob nicht registrierte Geräte abgewiesen werden.

Nachweise Konfiguration der Zugriffsregeln, Liste registrierter Geräte

Schritt 03 — BSI SYS.2.1; ISO/IEC 27001:2022 Anhang A 8.9

Endgeräte werden mit einer gehärteten Standardkonfiguration ausgerollt; Abweichungen werden erkannt.

Prüfhandlung Standardkonfiguration ansehen und auf fünf Geräten zentrale Einstellungen wie Firewall, Bildschirmsperre und Autostart auslesen.

Nachweise Konfigurationsvorgabe, Gruppenrichtlinien oder Profile, Auslesung der Stichprobe

Prüfschritte 4 bis 6

Schritt 04 ISO/IEC 27001:2022 Anhang A 8.7; BSI OPS.1.1.4

Ein Schutz vor Schadprogrammen ist auf allen Geräten aktiv, aktuell und meldet Funde zentral.

Prüfhandlung Zentrale Konsole auswerten: Abdeckung, Signaturstand und Geräte ohne Meldung in den letzten sieben Tagen.

Nachweise Bericht der Schutzlösung zu Abdeckung und Status, Fundliste

Schritt 05 ISO/IEC 27001:2022 Anhang A 8.8

Betriebssystem und Anwendungen werden zeitnah aktualisiert; nicht aktualisierte Geräte werden nachverfolgt.

Prüfhandlung Patchstand der Endgeräte aus dem Verteilwerkzeug auswerten und die Behandlung von Nachzüglern nachvollziehen.

Nachweise Patchbericht, Liste nicht aktueller Geräte mit Maßnahmen

Schritt 06 BSI SYS.3.1; ISO/IEC 27001:2022 Anhang A 8.24

Datenträger von Laptops und mobilen Geräten sind vollständig verschlüsselt, Wiederherstellungsschlüssel sind sicher hinterlegt.

Prüfhandlung Verschlüsselungsstatus aus der Verwaltungskonsole abrufen und den Zugriff auf Wiederherstellungsschlüssel prüfen.

Nachweise Verschlüsselungsbericht, Berechtigungen auf die Schlüsselablage

Prüfschritte 7 bis 9

Schritt 07

BSI SYS.3.2.2; BSI SYS.3.2.1

Das Mobile Device Management setzt Vorgaben wie Gerätesperre, Verschlüsselung und Mindestversion des Betriebssystems durch.

Prüfhandlung Profile und Konformitätsregeln im MDM ansehen und nicht konforme Geräte mit ihrer Behandlung nachvollziehen.

Nachweise MDM-Profile, Konformitätsbericht, Liste nicht konformer Geräte

Schritt 08

BSI SYS.3.2.1; ISO/IEC 27001:2022 Anhang A 8.1

Dienstliche und private Daten sind auf mobilen Geräten getrennt; die Nutzung privater Geräte ist geregelt.

Prüfhandlung Regelung zu privaten Geräten lesen und die technische Trennung (Container, App-Schutzrichtlinien) an einem Gerät vorführen lassen.

Nachweise Regelung zur Nutzung privater Geräte, Konfiguration der App-Schutzrichtlinien

Schritt 09

ISO/IEC 27001:2022 Anhang A 8.2 und 8.19

Lokale Administratorrechte sind eingeschränkt; Nutzer können Software nur über freigegebene Wege installieren.

Prüfhandlung Mitglieder der lokalen Administratorgruppen auf einer Stichprobe auslesen und Ausnahmen mit Begründung abgleichen.

Nachweise Auslesung lokaler Gruppen, Ausnahmeliste mit Genehmigungen

Prüfschritte 10 bis 12

Schritt 10

ISO/IEC 27001:2022 Anhang A 7.10; BSI SYS.4.5

Die Nutzung von Wechseldatenträgern ist geregelt und technisch eingeschränkt.

Prüfhandlung Regelung lesen und die technische Sperre oder Freigabeliste für Wechseldatenträger auf einem Gerät prüfen.

Nachweise Regelung zu Wechseldatenträgern, Gerätesteuerungsrichtlinie

Schritt 11

BSI SYS.3.2.2; ISO/IEC 27001:2022 Anhang A 6.8

Verlorene oder gestohlene Geräte werden unverzüglich gemeldet, gesperrt und bei Bedarf aus der Ferne gelöscht.

Prüfhandlung Für drei Verlustmeldungen der letzten zwölf Monate Meldung, Sperre und Fernlöschung mit Zeitstempeln nachvollziehen.

Nachweise Verlustmeldungen, Protokoll der MDM-Aktionen, Vorfallstickets

Schritt 12

ISO/IEC 27001:2022 Anhang A 5.11 und 7.14

Bei Austritt oder Aussonderung werden Geräte zurückgenommen und vor Wiederverwendung sicher gelöscht.

Prüfhandlung Fünf Austritte auswählen und Rückgabe sowie Löschung der Geräte nachvollziehen.

Nachweise Rückgabeprotokolle, Löschnachweise

Unterlagenanforderung

Diese 8 Unterlagen vor Prüfungsbeginn anfordern

1. Endgeräterichtlinie und Regelung zu privaten Geräten
2. Standardkonfiguration je Betriebssystem
3. Bericht der Schutzlösung gegen Schadprogramme
4. Patchbericht der Endgeräte
5. Verschlüsselungsbericht
6. MDM-Profile und Konformitätsbericht
7. Ausnahmeliste für lokale Administratorrechte
8. Verlustmeldungen und Protokoll der Fernlöschungen

TYPISCHE FESTSTELLUNGEN

- Ein Teil der Geräte meldet sich seit Wochen nicht mehr bei der Schutzlösung.
- Nutzer haben dauerhaft lokale Administratorrechte ohne Begründung.
- Laptops sind nicht durchgängig verschlüsselt, Wiederherstellungsschlüssel liegen ungeschützt.
- Private Geräte greifen ohne Registrierung auf E-Mail und Dateien zu.
- Verlorene Geräte werden spät gemeldet und nicht aus der Ferne gelöscht.
- Zurückgegebene Geräte werden ohne Löschnachweis neu ausgegeben.

Bibliothek Muster-Prüfprogramme

29 Muster-Prüfprogramme online

proauditmap.com/pruefprogramme/

Vollständiges Prüfpaket in ProAuditMap

proauditmap.com

ProAuditMap

Muster ohne Gewähr und keine Rechtsberatung. Gesetze, Verordnungen und Standards erscheinen nur als Fundstelle, Normtexte sind nicht abgedruckt. Passen Sie Umfang und Tiefe vor der Verwendung an Ihre Organisation, Ihre Risiken und die aktuelle Fassung der für Sie geltenden Vorschriften an. Stand: 13. Oktober 2026