Richtlinien

- Policy – Informationssicherheit
- Policy – Datenklassifizierung & Schutzbedarf
- Policy – Passwort & MFA
- Policy – Zugriff & Berechtigungen (IAM)
- Policy – Logging & Aufbewahrung

Policy – Informationssicherheit

Informationssicherheits-Policy

Version: 1.0 | **Owner:** IT-Leitung | **Geltungsbereich:** Unternehmensweit

Ziel

Schutz von Vertraulichkeit, Integrität, Verfügbarkeit (VIA) auf Basis eines risikoorientierten Ansatzes.

Grundsätze

- Minimalprinzip (Least Privilege), MFA standard, Netzwerksegmentierung
- Härtung & Patchen, Protokollierung & Auswertung, Backup/BCM
- Sensibilisierung & Schulung, Lieferantensteuerung

Mindestanforderungen

- Passwort- & MFA-Vorgaben, Endgeräte-Verschlüsselung, Admin-Protokollierung
- Patchfenster & Schwachstellenbehebung
- Notfallmanagement inkl. Übungen

Verweise

- TOMs (Art. 32), Notfallhandbuch (BSI 200-4), GoBD-Verfahrensdoku, Patch/Vuln-Prozess

Policy – Datenklassifizierung & Schutzbedarf

Policy – Datenklassifizierung & Schutzbedarf

Klassen: Öffentlich · Intern · Vertraulich · Streng vertraulich
Kennzeichnung: Dokument-/System-Tags, Ordnerstruktur, Watermark (falls möglich)

Beispiele:

- *Vertraulich:* Mitarbeiter-, Kunden-, Finanzdaten
- *Intern:* Prozessdokumente, Betriebsanweisungen

Schutzbedarf: Auswirkung auf Vertraulichkeit, Integrität, Verfügbarkeit → Maßnahmen ableiten.

Policy – Passwort & MFA

Policy – Passwort & MFA

- **MFA** verpflichtend für Admins, Remote/VPN, Cloud
- **Passwörter:** ausreichend lang, Manager empfohlen, keine Wiederverwendung
- **Servicekonten:** Kennworttresor, Rotation, keine interaktive Anmeldung
- **Reset-Prozess:** Identitätsprüfung, Protokollierung

Policy – Zugriff & Berechtigungen (IAM)

Policy – Zugriff & Berechtigungen (IAM)

- Rollenbasiert (RBAC), **Need-to-know**
- Joiner-Mover-Leaver (JML) Prozess verbindlich
- Adminrechte nur temporär (Just-in-Time), Vier-Augen-Prinzip
- Regelmäßige Rezertifizierung (z. B. halbjährlich), Nachweise dokumentieren

Policy – Logging & Aufbewahrung

Policy – Logging & Aufbewahrung

Pflichtquellen: AD, Firewalls, VPN, kritische Server/Anwendungen
Inhalte: An-/Abmeldungen, Admin-Aktionen, Policy-Änderungen, Fehler/Eskalationen
Aufbewahrung: gem. Schutzbedarf/DSGVO/GoBD
Auswertung: Dashboards/Alerts (LibreNMS, Wazuh/OpenSearch/Graylog), Monatsreport als Nachweis