IT-Sicherheitskonzept

Ausfüllbare Vorlage für kleine Unternehmen, Arztpraxen und Kanzleien

So nutzen Sie diese Vorlage: Füllen Sie die Felder von oben nach unten aus. Sie brauchen kein IT-Fachwissen, gesunder Menschenverstand und Ehrlichkeit reichen. Was Sie nicht wissen, markieren Sie als offenen Punkt. Das Ergebnis ist ein prüfsicheres Grundgerüst nach DSGVO Art. 32. Rechtlich verbindlich wird es mit fachlicher Prüfung.

UNTERNEHMEN	STANDORT(E)
VERANTWORTLICH (NAME)	ERSTELLT AM / VERSION
NÄCHSTE ÜBERPRÜFUNG AM	

1 Geltungsbereich & Verantwortliche

Welche Standorte, Systeme und Personen deckt dieses Konzept ab? Wer ist zuständig (intern/extern)?

2 Inventar: Was haben wir?

Die wichtigsten Geräte, Server, Programme und Datenbestände. Ohne Inventar kein Schutz.

ASSET (GERÄT / PROGRAMM / DATEN)	ORT / VERANTWORTLICH	BEMERKUNG

3 Schutzbedarf: Was ist kritisch?

Wie schlimm ist es, wenn das Asset ausfällt, gestohlen wird oder verfälscht wird? (niedrig / mittel / hoch)

ASSET	VERFÜGBARKEIT	VERTRAULICHKEIT	INTEGRITÄT

4 Risiken: Was kann passieren?

RISIKO / BEDROHUNG	WAHRSCHEINLICHKEIT	GEGENMASSNAHME (SIEHE 5/6)
Ransomware / Verschlüsselung		
Ausfall Server / Hardware		
Diebstahl / Verlust Gerät		
Menschlicher Fehler / Phishing		

5 Technische Maßnahmen

Ankreuzen, was umgesetzt ist. Leere Kästchen sind Ihre To-do-Liste.

- ☐ **Backup nach 3-2-1** (3 Kopien, 2 Medien, 1 außer Haus) und mindestens einmal testweise zurückgespielt
- ☐ **Virenschutz / Endpoint-Schutz** aktiv und aktuell auf allen Geräten
- ☐ **Firewall** am Internetzugang, Fernzugriffe abgesichert
- ☐ **Updates** für Betriebssystem und Programme zeitnah eingespielt
- ☐ **Verschlüsselung** von Notebooks und mobilen Datenträgern
- ☐ **Mehr-Faktor-Anmeldung (MFA)** für E-Mail, Cloud und Fernzugriff
- ☐ **Netztrennung** (Gäste-WLAN getrennt, kritische Systeme isoliert)

6 Organisatorische Maßnahmen

- ☐ **Passwortregeln** (individuell pro Person, keine geteilten Zugänge, Passwortmanager)
- ☐ **Berechtigungen** nach Bedarf vergeben, regelmäßig geprüft
- ☐ **Onboarding/Offboarding** geregelt (Zugänge werden bei Austritt sofort entzogen)
- ☐ **Schulung / Sensibilisierung** des Teams (Phishing, Umgang mit Daten)
- ☐ **Mobile Geräte / Homeoffice** geregelt
- ☐ **Dienstleister / Auftragsverarbeitung** mit AV-Verträgen abgedeckt

7 Notfallplan

Eine halbe Seite genügt, im Ernstfall zählt Klarheit, nicht Länge.

Wen rufe ich an? (Reihenfolge, Nummern)

Wo liegt die letzte saubere Sicherung, und wie spiele ich sie zurück?

In welcher Reihenfolge fahren wir Systeme wieder hoch?

8 Prüfung & Aktualisierung

Ein Konzept, das niemand aktualisiert, veraltet.

DATUM	GEPRÜFT VON	ÄNDERUNGEN