PRAXISNAH
VERSTÄNDLICH
UMSETZBAR

IT-SICHERHEIT
VERSTÄNDLICH ERKLÄRT

PRAXISLEITFADEN

Umfassender Leitfaden
für Privatnutzer,
Selbstständige und
kleine Unternehmen

Schützen
Ihre Daten, Geräte
und Identität

Verstehen
Risiken, Angriffe und
Schwachstellen

Sichern
Backups, Passwörter
und wichtige Inhalte

Handeln
Praktische Schritt-für-Schritt-
Anleitungen und Checklisten

PRAKTISCH.
AKTUELL.
ALLTAGSTAUGLICH.

- 10 wichtigste Maßnahmen
- Phishing & Ransomware schützen
- Backups richtig umsetzen
- Netzwerk und Geräte absichern
- Checklisten und Quick Wins

IT Sicherheitscheckliste

1) Inhalt

2) Informationssicherheitsorganisation

2.1 Richtlinien & Governance

Prüfpunkte	erledigt
Informationssicherheitsrichtlinie dokumentiert und freigegeben	☐
Rollen und Verantwortlichkeiten definiert	☐
ISMS etabliert oder geplant	☐
Sicherheitsziele definiert	☐
Regelmäßige Management-Reviews durchgeführt	☐
Sicherheitsvorfälle dokumentiert und ausgewertet	☐

2.2 Risikomanagement

Prüfpunkte	erledigt
Schutzbedarfsanalyse durchgeführt	☐
Risiken identifiziert und bewertet	☐
Maßnahmenplan dokumentiert	☐
Regelmäßige Risikoüberprüfung etabliert	☐

3) Benutzer- und Berechtigungsmanagement

3.1 Benutzerkonten

Prüfpunkte	erledigt
Benutzerkonten eindeutig zugeordnet	☐
Keine gemeinsamen Benutzerkonten ohne Ausnahmegenehmigung	☐
Standardkonten und Administratorkonten getrennt	☐
Inaktive Konten deaktiviert	☐

3.2 Passwortrichtlinien

Prüfpunkte	erledigt
Mindestlänge definiert	□
Komplexitätsanforderungen umgesetzt	□
Passwortmanager empfohlen oder verpflichtend	□
MFA/2FA aktiviert	□

3.3 Berechtigungen

Prüfpunkte	erledigt
Least-Privilege-Prinzip umgesetzt	□
Regelmäßige Rechteprüfung durchgeführt	□
Berechtigungsänderungen dokumentiert	□
Sofortige Deaktivierung bei Austritt umgesetzt	□

4) Arbeitsplatzsicherheit

4.1 Endgeräte

Prüfpunkte	erledigt
Aktuelle Betriebssysteme eingesetzt	☐
Sicherheitsupdates automatisiert	☐
Virenschutz/EDR aktiv	☐
Festplattenverschlüsselung aktiviert	☐
Bildschirmsperre konfiguriert	☐

4.2 Mobile Geräte

Prüfpunkte	erledigt
Mobile Device Management vorhanden	☐
PIN/Biometrie verpflichtend	☐
Remote-Wipe möglich	☐
Trennung privat/geschäftlich geregelt	☐

4.3 Homeoffice

Prüfpunkte	erledigt
Sichere VPN-Nutzung etabliert	☐
WLAN-Sicherheit geprüft	☐
Clean-Desk-Regel bekannt	☐
Sensible Dokumente geschützt	☐

5) Netzwerksicherheit

5.1 Netzwerksegmentierung

Prüfpunkte	erledigt
Interne Netze segmentiert	☐
Gäste-WLAN getrennt	☐
Kritische Systeme isoliert	☐

5.2 Firewall & Zugriffsschutz

Prüfpunkte	erledigt
Firewall-Regeln dokumentiert	☐
Unnötige Ports deaktiviert	☐
Fernzugriffe abgesichert	☐
IDS/IPS vorhanden	☐

5.3 WLAN

Prüfpunkte	erledigt
WPA3 oder mindestens WPA2 aktiviert	☐
Standardpasswörter geändert	☐
Regelmäßige Schlüsselrotation definiert	☐

6) Server- und Systemhärtung

6.1 Betriebssysteme

Prüfpunkte	erledigt
Nicht benötigte Dienste deaktiviert	☐
Sicherheits-Baselines angewendet	☐
Lokale Adminrechte minimiert	☐

6.2 Patchmanagement

Prüfpunkte	erledigt
Patchprozess dokumentiert	☐
Kritische Updates priorisiert	☐
Testverfahren definiert	☐

6.3 Logging & Monitoring

Prüfpunkte	erledigt
Zentrale Protokollierung vorhanden	☐
Sicherheitsereignisse überwacht	☐
Alarmierung definiert	☐

7) 6. Datensicherung & Wiederherstellung

7.1 Backup

Prüfpunkte	erledigt
Backupstrategie dokumentiert	☐
Regelmäßige Sicherungen automatisiert	☐
Offsite-/Offline-Backups vorhanden	☐
Backupverschlüsselung aktiviert	☐

7.2 Wiederherstellung

Prüfpunkte	erledigt
Restore-Tests durchgeführt	☐
Wiederanlaufzeiten definiert	☐
Notfallhandbuch vorhanden	☐

---

8) 7. E-Mail- und Kommunikationssicherheit

8.1 E-Mail-Schutz

Prüfpunkte	erledigt
Spamfilter aktiv	☐
DKIM/SPF/DMARC eingerichtet	☐
Phishing-Schutzmaßnahmen etabliert	☐

8.2 Sensibilisierung

Prüfpunkte	erledigt
☐ Awareness-Schulungen durchgeführt	☐
☐ Phishing-Tests etabliert	☐
☐ Meldewege bekannt	☐

---

9) 8. Cloud- und SaaS-Sicherheit

9.1 Zugriff & Konfiguration

Prüfpunkte	erledigt
MFA für Cloud-Dienste aktiviert	☐
Rollenbasierte Berechtigungen umgesetzt	☐
Unsichere Freigaben überprüft	☐

9.2 Datensicherheit

Prüfpunkte	erledigt
Datenklassifizierung definiert	☐
Verschlüsselung aktiviert	☐
Backup der Cloud-Daten geregelt	☐

---

10) Datenschutz & Compliance

10.1 Datenschutz

Prüfpunkte	erledigt
Verzeichnis von Verarbeitungstätigkeiten vorhanden	☐
AV-Verträge abgeschlossen	☐
Löschkonzept definiert	☐
Datenschutzvorfälle dokumentiert	☐

10.2 Compliance

Prüfpunkte	erledigt
Relevante Normen identifiziert	☐
Gesetzliche Anforderungen geprüft	☐
Auditnachweise verfügbar	☐

11) Incident Response & Notfallmanagement

11.1 Sicherheitsvorfälle

Prüfpunkte	erledigt
Incident-Response-Prozess dokumentiert	☐
Eskalationswege definiert	☐
Ansprechpartner benannt	☐
Forensische Sicherung geregelt	☐

11.2 Notfallmanagement

Prüfpunkte	erledigt
☐ Business-Continuity-Plan vorhanden	☐
☐ Notfallkontakte aktuell	☐
☐ Übungen durchgeführt	☐

---

12) Lieferanten- und Drittparteimanagement

Prüfpunkte	erledigt
Sicherheitsanforderungen vertraglich geregelt	☐
Dienstleister bewertet	☐
Externe Zugriffe kontrolliert	☐
Regelmäßige Überprüfung durchgeführt	☐

---

13) Physische Sicherheit

Prüfpunkte	erledigt
Zutrittskontrolle vorhanden	□
Serverräume abgesichert	□
Brandschutz vorhanden	□
USV installiert	□
Besucherregelung definiert	□

---

14) Dokumentation & Nachweisführung

Prüfpunkte	erledigt
□ Sicherheitsdokumentation aktuell	□
□ Änderungen nachvollziehbar dokumentiert	□
□ Prüfprotokolle archiviert	□
□ Verantwortlichkeiten dokumentiert	□

---

15) Bewertungsschema (optional)

Status	Bedeutung
1 = Erfüllt	Maßnahme vollständig umgesetzt
2 = Teilweise erfüllt	Teilweise umgesetzt / Optimierung nötig
3 = Nicht erfüllt	Maßnahme fehlt
4 = Nicht relevant	Für Organisation nicht anwendbar

15.1 Reifegradbewertung (optional)

Bereich	Reifegrad 1–4
Organisation	
Identitätsmanagement	
Netzwerksicherheit	
Backup & Recovery	
Incident Response	
Awareness	
Compliance	

16) Freigabe und Revision

Rolle	Name	Datum	Unterschrift
Erstellt durch			
Geprüft durch			
Freigegeben durch			

Hinweise

Diese Checkliste dient als organisatorische und technische Mindestanforderung für Backup- und Wiederherstellungsprozesse im Rahmen eines Informationssicherheitsmanagementsystems (ISMS). Die konkreten Anforderungen sind an Schutzbedarf, Unternehmensgröße sowie regulatorische Vorgaben anzupassen.

17) Impressum

Herausgeber:
MINCOM GmbH
Unterhachinger Straße 55
85521 Ottobrunn
www.mincom.de

Geschäftsleitung:
Dr. Rainer Wittmann