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) Informationssicherheitsorganisation

1.1 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	☐

1.2 Risikomanagement

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

2) Benutzer- und Berechtigungsmanagement

2.1 Benutzerkonten

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

2.2 Passwortrichtlinien

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

2.3 Berechtigungen

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

3) Arbeitsplatzsicherheit

3.1 Endgeräte

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

3.2 Mobile Geräte

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

3.3 Homeoffice

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

4) Netzwerksicherheit

4.1 Netzwerksegmentierung

- □ Interne Netze segmentiert
- □ Gäste-WLAN getrennt
- □ Kritische Systeme isoliert

4.2 Firewall & Zugriffsschutz

- □ Firewall-Regeln dokumentiert
- □ Unnötige Ports deaktiviert
- □ Fernzugriffe abgesichert
- □ IDS/IPS vorhanden

4.3 WLAN

- □ WPA3 oder mindestens WPA2 aktiviert
- □ Standardpasswörter geändert
- □ Regelmäßige Schlüsselrotation definiert

---

5. Server- und Systemhärtung

Betriebssysteme

- □ Nicht benötigte Dienste deaktiviert
- □ Sicherheits-Baselines angewendet
- □ Lokale Adminrechte minimiert

Patchmanagement

- □ Patchprozess dokumentiert
- □ Kritische Updates priorisiert
- □ Testverfahren definiert

Logging & Monitoring

- □ Zentrale Protokollierung vorhanden
- □ Sicherheitsereignisse überwacht
- □ Alarmierung definiert

---

6. Datensicherung & Wiederherstellung

Backup

- □ Backupstrategie dokumentiert
- □ Regelmäßige Sicherungen automatisiert
- □ Offsite-/Offline-Backups vorhanden
- □ Backupverschlüsselung aktiviert

Wiederherstellung

- □ Restore-Tests durchgeführt
- □ Wiederanlaufzeiten definiert
- □ Notfallhandbuch vorhanden

---

7. E-Mail- und Kommunikationssicherheit

E-Mail-Schutz

- □ Spamfilter aktiv
- □ DKIM/SPF/DMARC eingerichtet
- □ Phishing-Schutzmaßnahmen etabliert

Sensibilisierung

- □ Awareness-Schulungen durchgeführt
- □ Phishing-Tests etabliert
- □ Meldewege bekannt

---

8. Cloud- und SaaS-Sicherheit

Zugriff & Konfiguration

- □ MFA für Cloud-Dienste aktiviert
- □ Rollenbasierte Berechtigungen umgesetzt
- □ Unsichere Freigaben überprüft

Datensicherheit

- □ Datenklassifizierung definiert
- □ Verschlüsselung aktiviert
- □ Backup der Cloud-Daten geregelt

---

9. Datenschutz & Compliance

Datenschutz

- □ Verzeichnis von Verarbeitungstätigkeiten vorhanden
- □ AV-Verträge abgeschlossen
- □ Löschkonzept definiert
- □ Datenschutzvorfälle dokumentiert

Compliance

- □ Relevante Normen identifiziert
- □ Gesetzliche Anforderungen geprüft
- □ Auditnachweise verfügbar

---

10. Incident Response & Notfallmanagement

Sicherheitsvorfälle

- □ Incident-Response-Prozess dokumentiert
- □ Eskalationswege definiert
- □ Ansprechpartner benannt
- □ Forensische Sicherung geregelt

Notfallmanagement

- □ Business-Continuity-Plan vorhanden
- □ Notfallkontakte aktuell
- □ Übungen durchgeführt

---

11. Lieferanten- und Drittparteimanagement

- □ Sicherheitsanforderungen vertraglich geregelt
- □ Dienstleister bewertet
- □ Externe Zugriffe kontrolliert
- □ Regelmäßige Überprüfung durchgeführt

---

12. Physische Sicherheit

- □ Zutrittskontrolle vorhanden
- □ Serverräume abgesichert
- □ Brandschutz vorhanden
- □ USV installiert
- □ Besucherregelung definiert

---

13. Dokumentation & Nachweisführung

- □ Sicherheitsdokumentation aktuell
- □ Änderungen nachvollziehbar dokumentiert
- □ Prüfprotokolle archiviert
- □ Verantwortlichkeiten dokumentiert

4.4 Bewertungsschema (optional)

Status	Bedeutung
Erfüllt	Maßnahme vollständig umgesetzt
Teilweise erfüllt	Teilweise umgesetzt / Optimierung nötig
Nicht erfüllt	Maßnahme fehlt
Nicht relevant	Für Organisation nicht anwendbar

4.5 Reifegradbewertung (optional)

Bereich	Reifegrad 1–5
Organisation	
Identitätsmanagement	
Netzwerksicherheit	
Backup & Recovery	
Incident Response	
Awareness	
Compliance	

5) 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.

6) Impressum

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

Geschäftsleitung:
Dr. Rainer Wittmann