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

Backup Checklist

Inhalt

1 Ziel der Datensicherung

Die Datensicherung dient dem Schutz vor:

- Hardwareausfällen
- Bedienfehlern
- Schadsoftware und Ransomware
- Diebstahl
- Brand-, Wasser- und Umweltschäden
- Datenkorruption
- Sabotage

Ziel ist die Wiederherstellbarkeit geschäftskritischer Daten und Systeme innerhalb definierter Wiederanlaufzeiten.

2 Organisatorische Anforderungen

Prüfpunkte	Erledigt
Backup-Verantwortlicher benannt	☐
Vertretungsregelung definiert	☐
Backup-Konzept dokumentiert	☐
Verantwortlichkeiten schriftlich festgelegt	☐
Wiederherstellungsziele (RTO/RPO) definiert	☐
Aufbewahrungsfristen festgelegt	☐
Notfallkontakte dokumentiert	☐
Backup-Prozesse in ISMS integriert	☐
Regelmäßige Review-Termine definiert	☐

3 Schutzbedarfs- und Datenklassifizierung

Prüfpunkte	Erledigt
Kritische Systeme identifiziert	☐
Geschäftskritische Daten klassifiziert	☐
Systeme mit hohem Schutzbedarf dokumentiert	☐
Gesetzliche Aufbewahrungspflichten berücksichtigt	☐
Personenbezogene Daten berücksichtigt	☐
Cloud-Dienste berücksichtigt	☐
Mobile Geräte berücksichtigt	☐

4 Technische Backup-Strategie

4.1 Backup-Arten

Prüfpunkte	Erledigt
Vollbackup definiert	☐
Inkrementelles Backup eingerichtet	☐
Differenzielles Backup bewertet	☐
Snapshot-Mechanismen geprüft	☐
Systemabbilder vorhanden	☐
Datenbank-Backups integriert	☐

4.2 Backup-Umfang

Prüfpunkte	Erledigt
Server gesichert	☐
Virtuelle Maschinen gesichert	☐
Datenbanken gesichert	☐
NAS-/Storage-Systeme gesichert	☐
Arbeitsplatzdaten berücksichtigt	☐
E-Mail-Systeme gesichert	☐
Cloud-Daten gesichert	☐
Konfigurationsdaten gesichert	☐
Netzwerkgeräte-Konfigurationen exportiert	☐

4.3 3-2-1-Regel

Prüfpunkte	Erledigt
Mindestens 3 Datenkopien vorhanden	☐
Speicherung auf 2 unterschiedlichen Medien	☐
Mindestens 1 Backup extern/offsite	☐
Offline-/Air-Gap-Backup vorhanden	☐
Immutable Backup geprüft/eingerichtet	☐

5 Backup-Sicherheit

Prüfpunkte	Erledigt
Backup-Daten verschlüsselt	☐
Backup-Übertragung verschlüsselt	☐
Zugriffsschutz eingerichtet	☐
Rollen- und Berechtigungskonzept vorhanden	☐
MFA für Backup-System aktiviert	☐
Backup-Netzwerk segmentiert	☐
Schutz vor Ransomware implementiert	☐
Backup-Server gehärtet	☐
Backup-Protokolle überwacht	☐

6 Aufbewahrung und Rotation

Prüfpunkte	Erledigt
Aufbewahrungsfristen definiert	☐
Generationenkonzept vorhanden	☐
Medienrotation dokumentiert	☐
Archivierung berücksichtigt	☐
Löschkonzept vorhanden	☐
DSGVO-Anforderungen berücksichtigt	☐

7 Wiederherstellung und Tests

Prüfpunkte	Erledigt
Restore-Tests regelmäßig durchgeführt	☐
Testintervalle definiert	☐
Vollständige Desaster-Recovery getestet	☐
Wiederherstellungszeiten dokumentiert	☐
Einzeldatei-Restore getestet	☐
Bare-Metal-Recovery getestet	☐
Restore-Dokumentation vorhanden	☐
Testergebnisse protokolliert	☐

8 Monitoring und Protokollierung

Prüfpunkte	Erledigt
Backup-Jobs werden überwacht	☐
Fehlerbenachrichtigungen eingerichtet	☐
Monitoring automatisiert	☐
Logs zentral gespeichert	☐
Backup-Kapazitäten überwacht	☐
Erfolgsquoten ausgewertet	☐

9 Notfallvorsorge

Prüfpunkte	Erledigt
Notfallhandbuch vorhanden	☐
Eskalationswege definiert	☐
Ansprechpartner dokumentiert	☐
Ersatzhardware berücksichtigt	☐
Wiederanlaufpläne dokumentiert	☐
Business-Continuity-Anforderungen berücksichtigt	☐

9.1 Compliance und Standards

Prüfpunkte	Erledigt
Anforderungen gemäß DSGVO berücksichtigt	☐
Anforderungen gemäß BSI IT-Grundschutz berücksichtigt	☐
Anforderungen gemäß ISO 27001 berücksichtigt	☐
Branchenvorgaben berücksichtigt	☐
Auditfähigkeit sichergestellt	☐
Dokumentation revisionssicher	☐

9.2 Empfohlene Mindestintervalle

Bereich	Empfehlung
Kritische Daten	täglich
Server-Systeme	täglich
Datenbanken	täglich bis stündlich
Konfigurationsdaten	nach Änderungen
Restore-Tests	mindestens vierteljährlich
Desaster-Recovery-Test	mindestens jährlich
Review Backup-Konzept	jährlich

9.3 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.

10 Impressum

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

Geschäftsleitung:
Dr. Rainer Wittmann