Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Sozialversicherungen BSV

Checkliste für IT-Sicherheit und Cyberprävention

Datum:	16.05.2025 / Mma, Bmu
Themengebiet:	Informationssicherheit und Datenschutz in der 1. Säule

Hinweis: Die nachfolgende Checkliste stellt eine unverbindliche Sammlung bewährter Massnahmen zur Erhöhung der IT-Sicherheit und Prävention von Cybervorfällen dar. Sie erhebt keinen Anspruch auf Vollständigkeit. Die Auswahl, Priorisierung und Umsetzung der genannten allgemeinen Empfehlungen sowie weiterer geeigneter Massnahmen obliegt der jeweiligen Durchführungsstelle unter Berücksichtigung individueller Gegebenheiten, Risiken und rechtlicher Anforderungen. Die Checkliste soll den Durchführungsstellen als Orientierungshilfe dienen, um geeignete Sicherheitsmassnahmen zu identifizieren und umzusetzen. Die Umsetzung dieser Massnahmen stellt keine Garantie gegen Sicherheitsvorfälle dar und erfolgt auf eigene Verantwortung.

1. Sicherung der Daten (Backup-Strategie)
(Rz 2.12, 2.17 W-ISDS)

- ☐ Tägliche automatische Backups einrichten.
- ☐ Immutable Backups einrichten: Sicherungen, die nicht gelöscht, verändert oder verschlüsselt werden können.
- ☐ Backup-Scanning aktivieren, um schadhafte Dateien und Ransomware zu erkennen.
- ☐ Backups ausserhalb des Netzwerks aufbewahren, idealerweise auf einem nicht verbundenen (offline) Medium. Dabei die 3-2-1-Regel beachten: 3 Kopien der Daten (Original + 2 Backups), auf zwei verschiedenen Medien, davon 1 Kopie an einem externen Ort (z. B. Cloud oder anderes Rechenzentrum).
- ☐ Backup regelmässig überprüfen, ob darauf zugegriffen werden kann.
- ☐ Wiederherstellung regelmässig testen, mindestens zweimal pro Jahr.

2. Absicherung der Endgeräte, Server und Anwendungen (Endpoint Security)
(Rz 2.3, 2.6, 2.12 W-ISDS)

- ☐ Virenschutz und Malware-Erkennung stets aktuell halten.
- ☐ EDR-Systeme (Endpoint Detection and Response) implementieren, um Endgeräte und Server kontinuierlich auf Bedrohungen zu überwachen.
- ☐ Updates & Patches: Sicherstellen, dass alle Software- und Hardwarekomponenten (Betriebssysteme, Anwendungen, Firmware, Treiber) regelmässig aktualisiert werden, um Sicherheitslücken zu schliessen und Schutz vor bekannten sowie künftigen Bedrohungen zu gewährleisten.
- ☐ Firewalls konfigurieren und Systeme absichern, z. B. unnötige Dienste deaktivieren und nicht verwendete Ports schliessen.
- ☐ Lokale Administratorrechte auf Clients entfernen («Least Privilege Principle»: Benutzer sollen nur die minimal erforderlichen Rechte haben).
- ☐ Richtlinie (Policy) zum Umgang mit Benutzerrechten definieren, um unerlaubte Installationen und das Anschliessen nicht genehmigter Geräte zu verbieten.
- ☐ Keine Geschäftsdaten lokal auf Endgeräten speichern.

- [ ] Geräteverschlüsselung (z. B. BitLocker) aktivieren, um gespeicherte Daten vor unbefugtem Zugriff zu schützen.
- [ ] Mobile Device Management (MDM) bzw. Mobile Application Management (MAM) für Bring-your-own-Devices (BYOD) und mobile Geräte einführen, um Sicherheit und Kontrolle über Daten auf privaten und mobilen Endgeräten sicherzustellen.

3. Zugriffssteuerung und Identitätsschutz (Access Control)
(Rz 2.9 W-ISDS)

- [ ] Starke Passwörter, Multi-Faktor-Authentifizierung (MFA) und standortbasierte, resp. adaptive Authentifizierung verwenden.
- [ ] Benutzerrechte regelmässig überprüfen: Nur aktive Benutzer mit minimal erforderlichen Rechten (gemäss «Least Privilege Principle») zulassen; nicht mehr benötigte Konten entfernen oder bis zur Löschung deaktivieren.
- [ ] Rollenbasierte Zugriffskontrollen (RBAC, Role-Based-Access Control) umsetzen und Benutzer nach ihren Aufgaben den entsprechenden Berechtigungsgruppen zuordnen.

4. Netzwerksicherheit und geschützte Informationsübertragung
(Rz 2.13 W-ISDS)

- [ ] Netzwerksegmentierung umsetzen, um kritische Systeme zu isolieren, den Datenverkehr gezielt zu kontrollieren und die Ausbreitung von Angriffen zu verhindern.
- [ ] Firewalls sowie IDS/IPS (Intrusion Detection/Prevention Systems) im Netzwerk einrichten, um unerwünschten Datenverkehr zu blockieren, Angriffsversuche zu erkennen und zu verhindern.
- [ ] XDR-System (Extended Detection and Response) implementieren, um den Netzwerkverkehr zu überwachen.
- [ ] VPN-Zugang mit MFA absichern oder Zero Trust Network Access (ZTNA) einführen.
- [ ] DNS-Sicherheitsdienste einsetzen, z. B. BACS «DNS-Firewall oder «Quad9».
- [ ] TLS (Transport Layer Security) konsequent einsetzen, um die Vertraulichkeit und Integrität der Datenübertragung zu gewährleisten; veraltete Protokolle oder unsichere TLS-Versionen (z. B. 1.0/1.1) deaktivieren.
- [ ] Geschützte Informationsübertragung sicherstellen, z. B. mit Sedex.

5. Monitoring und Alarmierung (Alerting)
(Rz 2.12 W-ISDS)

- [ ] Netzwerkverkehr in Echtzeit überwachen (z. B. mit IDS/IPS-Systeme).
- [ ] Benachrichtigungskanäle für Alarme definieren, um sicherzustellen, dass IT- und Sicherheitsteams im Falle eines Sicherheitsvorfalls sofort informiert werden.
- [ ] Log-Dateien regelmässig auf Auffälligkeiten und potenzielle Fehlalarme (False Positives) prüfen sowie Alarmierungsregeln optimieren.
- [ ] SIEM-System (Security Information and Event Management) einführen, um eine zentralisierte Analyse von Sicherheitsereignissen aus verschiedenen Quellen zu ermöglichen und die Reaktionszeit auf Vorfälle zu verkürzen.

6. Awareness, Rollen und Prozesse
(Rz 2.4, 2.7.2, 2.16, 2.17 W-ISDS)

- ☐ Alle Mitarbeitende regelmässig schulen, testen und sensibilisieren (Phishing, Social Engineering).
- ☐ Kontaktlisten für den Krisenfall aktuell halten und bereitstellen.
- ☐ Notfall-, Störungs- und Katastrophenpläne dokumentieren, aktuell halten und regelmässig testen, sowie Verantwortlichkeiten und Rollen klar definieren und in Übungen überprüfen.

7. Microsoft 365 (M365)
(Rz 2.15.2 W-ISDS)

- ☐ Multi-Faktor-Authentifizierung (MFA) für alle Benutzer und Administratoren aktivieren.
- ☐ Geo-IP-Blocking über «Conditional Access Named Locations» einrichten.
- ☐ Mindestens die Sicherheitsstufe «Standard» aktivieren.
- ☐ Neue Microsoft-Sicherheitsfunktionen regelmässig prüfen und aktivieren, um den Schutz kontinuierlich zu verbessern.

8. Verträge mit Dritten
(Rz 2.15.1 W-ISDS)

- ☐ Sicherstellen, dass Vertragspartner (Leistungserbringer) definierte Sicherheitsanforderungen erfüllen und deren Umsetzung nachweisen können.

Dieses Dokument finden Sie unter
https://sozialversicherungen.admin.ch/de/f/20762

Kontakt
Bundesamt für Sozialversicherungen BSV
IT Management
isms@bsv.admin.ch