Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'intérieur DFI
Office fédéral des assurances sociales OFAS

Liste de contrôle pour la sécurité informatique et la cyber prévention

Date :	16.05.2025 / Mma, Bmu
Domaine(s) :	Sécurité de l'information et protection des données dans le 1er pilier

Remarque : La liste de contrôle suivante constitue un recueil non contraignant de mesures éprouvées pour renforcer la sécurité informatique et prévenir les cyber-incidents. Elle ne prétend pas être exhaustive. Le choix, la hiérarchisation et la mise en œuvre des recommandations générales mentionnées ainsi que d'autres mesures appropriées incombent à chaque organe d'exécution, en tenant compte des circonstances individuelles, des risques et des exigences juridiques. La liste de contrôle doit servir de guide aux organes d'exécution pour identifier et mettre en œuvre des mesures de sécurité appropriées. La mise en œuvre de ces mesures ne constitue pas une garantie contre les incidents de sécurité et relève de la responsabilité de chacun.

1. Sauvegarde des données (stratégie de sauvegarde)
(ch. 2.12, 2.17 D-SIPD)

- ☐ Mettre en place des sauvegardes automatiques quotidiennes.
- ☐ Configurer des sauvegardes immuables : des sauvegardes qui ne peuvent être ni supprimées, ni modifiées, ni chiffrées.
- ☐ Activer l'analyse des sauvegardes pour détecter les fichiers malveillants et les ransomwares.
- ☐ Conserver les sauvegardes en dehors du réseau, idéalement sur un support non connecté (offline). Ce faisant, respecter la règle 3-2-1 : 3 copies des données (original + 2 sauvegardes), sur deux supports différents, dont 1 copie dans un lieu externe (par ex. cloud ou autre centre de données).
- ☐ Vérifier régulièrement si les sauvegardes sont accessibles.
- ☐ Tester régulièrement la restauration des sauvegardes, au moins deux fois par an.

2. Sécurisation des terminaux, des serveurs et des applications (Endpoint Security)
(ch. 2.3, 2.6, 2.12 D-SIPD)

- ☐ Maintenir la protection antivirus et la détection de logiciels malveillants à jour.
- ☐ Mettre en œuvre des systèmes EDR (Endpoint Detection and Response) pour surveiller en permanence les terminaux et les serveurs afin de détecter les menaces.
- ☐ Mises à jour et correctifs : s'assurer que tous les composants logiciels et matériels (systèmes d'exploitation, applications, micrologiciels, pilotes) sont régulièrement mis à jour afin de combler les failles de sécurité et d'assurer une protection contre les menaces connues et à venir.
- ☐ Configurer les pare-feu et sécuriser les systèmes, par ex. désactiver les services inutiles et fermer les ports non utilisés.
- ☐ Supprimer les droits d'administrateur local sur les postes clients (« Least Privilege Principle » : les utilisateurs ne doivent avoir que les droits minimums nécessaires).

- ☐ Définir une politique de gestion des droits des utilisateurs afin d'interdire les installations non autorisées et la connexion d'appareils non autorisés.
- ☐ Ne pas stocker de données professionnelles localement sur les terminaux.
- ☐ Activer le cryptage des appareils (par ex. BitLocker) pour protéger les données enregistrées contre tout accès non autorisé.
- ☐ Mettre en place une gestion des appareils mobiles (Mobile Device Management, MDM) ou une gestion des applications mobiles (Mobile Application Management, MAM) pour les appareils personnels apportés par les utilisateurs (Bring-your-own-Devices, BYOD) et les appareils mobiles afin d'assurer la sécurité et le contrôle des données, assurer le contrôle des données sur les terminaux privés et mobiles.

3. Contrôle d'accès et protection de l'identité (Access Control)
(ch. 2.9 D-SIPD)

- ☐ Utiliser des mots de passe forts, l'authentification multi-facteurs (MFA) et l'authentification basée sur la localisation, respectivement l'authentification adaptative.
- ☐ Vérifier régulièrement les droits des utilisateurs : N'autoriser que les utilisateurs actifs disposant des droits minimaux requis (selon le « Least Privilege Principle ») ; supprimer les comptes qui ne sont plus nécessaires ou les désactiver jusqu'à leur suppression.
- ☐ Mettre en œuvre des contrôles d'accès basés sur les rôles (RBAC, Role-Based-Access Control) et affecter les utilisateurs aux groupes d'autorisation correspondants en fonction de leurs tâches.

4. Sécurité des réseaux et transmission sécurisée des informations
(ch. 2.13 D-SIPD)

- ☐ Mettre en œuvre la segmentation du réseau pour isoler les systèmes critiques, contrôler le trafic de données de manière ciblée et prévenir la propagation des attaques.
- ☐ Mettre en place des pare-feu ainsi que des systèmes IDS/IPS (Intrusion Detection/Prevention Systems) sur le réseau afin de bloquer le trafic indésirable, de détecter et d'empêcher les tentatives d'attaque
- ☐ Mettre en œuvre le système XDR (Extended Detection and Response) pour surveiller le trafic réseau.
- ☐ Sécuriser l'accès VPN avec MFA ou introduire un Zero Trust Network Access (ZTNA).
- ☐ Utiliser des services de sécurité DNS, par ex. « Pare-feu DNS » de l’OFCS ou « Quad9 ».
- ☐ Utiliser systématiquement TLS (Transport Layer Security) pour assurer la confidentialité et garantir l'intégrité de la transmission des données ; désactiver les protocoles obsolètes ou les versions TLS non sécurisées (par ex. 1.0/1.1).
- ☐ Assurer une transmission protégée des informations, par ex. avec Sedex.

5. Suivi et alerte (Alerting)
(ch. 2.12 D-SIPD)

- ☐ Surveiller le trafic réseau en temps réel (par ex. avec des systèmes IDS/IPS).
- ☐ Définir des canaux de notification pour les alertes afin de garantir que les équipes informatiques et les équipes de sécurité soient immédiatement informées en cas d'incident de sécurité.
- ☐ Rechercher régulièrement des anomalies et des fausses alertes potentielles dans les fichiers log (faux positifs) et optimiser les règles d'alerte.
- ☐ Introduire un système SIEM (Security Information and Event Management) afin de permettre une analyse centralisée des événements de sécurité provenant de différentes sources et de réduire le temps de réaction aux incidents.

6. Sensibilisation, rôles et processus
(ch. 2.4, 2.7.2, 2.16, 2.17 D-SIPD)

- ☐ Former, tester et sensibiliser régulièrement tous les collaborateurs (Phishing, Social Engineering).
- ☐ Tenir à jour et mettre à disposition des listes de contacts en cas de crise.
- ☐ Documenter les plans d'urgence, de perturbation et de catastrophe, les tenir à jour et les tester régulièrement, ainsi que définir clairement les responsabilités et les rôles et les vérifier lors d'exercices.

7. Microsoft 365 (M365)
(ch. 2.15.2 D-SIPD)

- ☐ Activer l'authentification multi-facteurs (MFA) pour tous les utilisateurs et administrateurs.
- ☐ Configurer le géo-blocage IP via « Conditional Access Named Locations ».
- ☐ Activer au moins le niveau de sécurité « Standard ».
- ☐ Vérifier et activer régulièrement les nouvelles fonctions de sécurité Microsoft afin d'améliorer continuellement la protection.

8. Contrats avec des tiers
(ch. 2.15.1 D-SIPD)

- ☐ S'assurer que les partenaires contractuels (prestataires de services) remplissent des exigences de sécurité définies et qu'ils peuvent prouver leur mise en œuvre.

Vous trouverez ce document sur
https://sozialversicherungen.admin.ch/fr/f/20762

Contact
Office fédéral des assurances sociales OFAS
IT Management
isms@bsv.admin.ch