Socle de sécurité Microsoft 365 pour PME suisses

Trente-cinq points pour vérifier la sécurité de votre environnement Microsoft 365, classés par domaine et par priorité. Nous les contrôlons lors de chaque audit chez les PME romandes. Cochez ce qui est en place : ce qui reste vide est votre feuille de route.

Identités et accès

- [ ] **Double authentification pour 100 % des comptes** — Urgent
  Authenticator ou clé d'accès. Le SMS de Microsoft disparaît à partir du 1er février 2027.
- [ ] **Entre deux et quatre administrateurs globaux** — Urgent
  Comptes nominatifs dédiés, séparés des comptes de travail, dont un compte d'accès d'urgence protégé par clé FIDO2.
- [ ] **Aucun compte générique d'ancien prestataire** — Urgent
  Supprimer ou désactiver les comptes « admin », « support » ou « it » hérités.
- [ ] **Authentification héritée bloquée** — Important
  Bloquer les anciens protocoles qui ne gèrent pas la double authentification (accès conditionnel ou paramètres de sécurité par défaut).
- [ ] **Réinitialisation du mot de passe en libre-service** — Important
  Configurée avec des méthodes autres que le SMS.
- [ ] **Comptes dormants et invités revus** — Important
  Comptes sans connexion depuis 90 jours désactivés, invités externes revus chaque trimestre.

Messagerie

- [ ] **Transferts automatiques vers l'extérieur bloqués** — Urgent
  Une règle de transfert ajoutée par un pirate est la première chose à chercher après un phishing.
- [ ] **Un seul enregistrement SPF, sous 10 recherches DNS** — Important
  Et aucun include vers une cible qui ne publie rien.
- [ ] **DKIM activé chez chaque émetteur** — Important
  Microsoft 365, outil d'e-mailing, logiciel de facturation : chacun signe avec sa propre clé.
- [ ] **DMARC publié avec des rapports, puis durci** — Important
  Commencer en p=none avec rua, durcir après lecture des rapports.
- [ ] **POP et IMAP désactivés s'ils ne servent pas** — Important
  Portes d'entrée fréquentes pour les attaques par mot de passe et les anciennes applications. Idem pour SMTP AUTH.
- [ ] **Journal d'audit Microsoft 365 activé** — Urgent
  Sans lui, impossible de reconstituer un incident. Conservation standard : 180 jours.

Applications et données partagées

- [ ] **Consentement des utilisateurs aux applications tierces restreint** — Urgent
  Un utilisateur ne doit pas pouvoir autoriser seul une application à lire les e-mails de toute l'entreprise.
- [ ] **Applications d'IA autorisées revues** — Important
  Lister les applications qui ont accès à la messagerie, aux fichiers et à Teams.
- [ ] **Partage externe SharePoint et OneDrive maîtrisé** — Important
  Liens « tout le monde » désactivés ou limités dans le temps.

Postes et téléphones

- [ ] **Systèmes et Office encore supportés** — Urgent
  Windows 10 (hors mises à jour étendues payantes), Office 2016 et Office 2019 ne reçoivent plus de correctifs depuis le 14 octobre 2025.
- [ ] **Protection EDR sur 100 % des postes** — Urgent
  Supervisé, avec des alertes qui arrivent chez quelqu'un.
- [ ] **Disques chiffrés** — Important
  BitLocker sur Windows, FileVault sur Mac, clés de récupération stockées dans Intune.
- [ ] **Téléphones encadrés** — Important
  Code de verrouillage et protection des données professionnelles exigés pour accéder à la messagerie.
- [ ] **Pas de droits administrateur pour les utilisateurs** — Important
  Et un seul outil de prise en main à distance, connu et contrôlé.
- [ ] **Mises à jour automatiques et suivies** — Important
  Postes, navigateurs et applications métier.

Sauvegarde et continuité

- [ ] **Microsoft 365 sauvegardé par un outil indépendant** — Urgent
  Messagerie, OneDrive, SharePoint et Teams. L'historique des versions n'est pas une sauvegarde.
- [ ] **Tous les serveurs dans les tâches de sauvegarde** — Urgent
  Contrôleur de domaine et serveur applicatif compris.
- [ ] **Une copie hors ligne ou immuable** — Urgent
  Sinon un rançongiciel chiffre aussi les sauvegardes.
- [ ] **Restauration testée et documentée** — Important
  Avec des objectifs écrits : perte de données acceptable et délai de remise en route.

- [ ] **Données et sauvegardes hébergées en Suisse** — Important
  Simplifie la conformité nLPD et les exigences de certains secteurs régulés, sans être une obligation légale générale.

Réseau

- [ ] **Pare-feu à jour, avec filtrage des menaces** — Important
  Firmware récent, journaux conservés.
- [ ] **Consoles d'administration sans identifiants d'usine** — Urgent
  Serveurs, pare-feu, imprimantes, NAS : aucun mot de passe par défaut.
- [ ] **Réseau segmenté** — Important
  Postes, serveurs, invités et objets connectés séparés.
- [ ] **VPN protégé par double authentification** — Important
  Attention : les clés d'accès ne fonctionnent pas avec les VPN qui passent par NPS/RADIUS, et le SMS disparaît en février 2027.

Gouvernance et humain

- [ ] **Inventaire du matériel et des comptes à jour** — Important
  On ne protège pas ce qu'on ne connaît pas.
- [ ] **Simulations de phishing et formation régulières** — Important
  Avec un suivi des résultats.
- [ ] **Procédure d'incident écrite** — Important
  Qui appeler, quoi couper, qui prévenir. Établissements FINMA : première annonce sous 24 heures. Infrastructures critiques : annonce à l'OFCS sous 24 heures.
- [ ] **Directive sur l'usage de l'IA** — Important
  Ce qui est autorisé, avec quels outils et quelles données.
- [ ] **Gestionnaire de mots de passe d'entreprise** — Important
  La fin des mots de passe réutilisés ou notés en clair.