

Les 13 contrôles de base pour PME

Source : Centre canadien pour la cybersécurité, v1.2 (février 2020) <https://www.cyber.gc.ca/fr/orientation/introduction-aux-contrôles-de-base> et PDF https://www.cyber.gc.ca/sites/default/files/cyber/publications/Baseline.Controls.SMO1_2-fr.pdf

- ☐ 3.1 Élaborer un plan d'intervention en cas d'incident
- ☐ 3.2 Appliquer automatiquement les correctifs aux systèmes
- ☐ 3.3 Activer les logiciels de sécurité : ex. Defender, <https://learn.microsoft.com/en-us/defender-office-365/preset-security-policies>
- ☐ 3.4 Configurer les dispositifs pour assurer leur sécurité
- ☐ 3.5 Utiliser une authentification forte : <https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults>
- ☐ 3.6 Sensibiliser les employés
- ☐ 3.7 Sauvegarder et chiffrer les données
- ☐ 3.8 Sécuriser les services mobiles
- ☐ 3.9 Établir un périmètre de défense de base
- ☐ 3.10 Sécuriser les services infonuagiques et les services de TI : <https://learn.microsoft.com/en-us/security/benchmark/azure/introduction>
- ☐ 3.11 Sécuriser les sites Web
- ☐ 3.12 Mettre en œuvre des contrôles d'accès et d'autorisation : <https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/best-practices>
- ☐ 3.13 Sécuriser les supports amovibles Libellés repris du PDF du Centre canadien pour la cybersécurité (section 3). Liens Microsoft : documentation officielle Microsoft Learn.