AIDE-MÉMOIRE

GÉRER LES ACCÈS ET LES MOTS DE PASSE

Objectif du document

Gérer ses accès et ses mots de passe de manière sécuritaire.

Un mot de passe volé ou une mauvaise utilisation des codes d'accès peuvent permettre à une personne mal intentionnée de consulter ou de voler l'information confidentielle, voire d'effectuer des opérations non autorisées sur un système de l'entreprise.

Ce document vous aidera à assurer une meilleure gestion des accès et à renforcer la sécurité de vos mots de passe.

Destinataire du document : Personne responsable de la sécurité des systèmes d'information

Date de la dernière modification : 2017-06

Gestion des accès

Création, modification, retrait et révision des accès

- Prévenir le responsable de la gestion des accès de l'arrivée, du changement de poste, du départ ou de l'absence prolongée d'un employé. Le gestionnaire doit s'assurer d'indiquer le poste qui sera occupé, les accès à octroyer et la date de prise d'effet du changement.
- S'assurer qu'un employé qui effectue une demande d'accès supplémentaire a bel et bien besoin des accès demandés dans le cadre de ses fonctions avant de les lui octroyer.
- Effectuer annuellement la vérification des comptes et des accès des employés pour les applications, afin que les gestionnaires s'assurent que les accès des employés sont encore justifiés par un besoin d'affaires.
- S'assurer que les codes d'accès sont personnels, c'est-à-dire qu'ils sont émis sur une base individuelle de sorte que chaque employé est responsable et imputable de l'usage qui est fait du code d'accès qu'il reçoit.
- Désactiver les accès pour toute absence prolongée supérieure à 2 semaines, excluant les vacances.
- Désactiver les codes d'accès et supprimer les accès aux applications ou aux projets dans les 10 jours suivant le départ d'un employé.

Sensibiliser les employés

- Sensibiliser, dès leur embauche, les employés internes et externes (ex. : les consultants) en matière d'utilisation des codes d'accès et de protection des mots de passe.

Mots de passe

Le mot de passe initial doit être communiqué à l'employé de façon sécuritaire (ex. : enveloppe scellée remise en main propre). Tout mot de passe initial octroyé doit être modifié à la première utilisation. Il est important de créer des mots de passe sécuritaires, car un mot de passe qui ne respecte pas les critères de sécurité peut être trouvé par des pirates informatiques en quelques minutes.

Utiliser des mots de passe complexes, d'un minimum de 10 caractères, respectant l'une de ces deux options :

- Option 1 : mot de passe incluant des lettres ou des chiffres choisis aléatoirement
    - Astuce : utiliser les premières lettres de chaque mot d'une phrase
    - Exemple : la phrase « Mon chien Fido est un caniche blanc de race pure » devient « mcfeucbdrp »
- Option 2 : mot de passe composé d'au moins 3 mots, excluant les mots à éviter
    - Exemple : tablefeuillemanger
    - Mots à éviter : mots associés à l'environnement immédiat, professionnel ou personnel Exemples : nom du conjoint, d'un enfant, du chien, marque de votre ordinateur ou de votre souris, pensée du jour affichée sur le babillard, saison, jour de la semaine, mois ou année

À ne pas faire

- Utiliser les exemples de mots de passe donnés sur cette page.
- Consigner les mots de passe dans un fichier Excel, sur un papillon adhésif, etc., sauf dans une voûte de mots de passe (ex. : 1Password, KeePass).
- Divulguer ses mots de passe à quiconque, que ce soit un collègue, un gestionnaire, un adjoint ou tout autre employé, ami ou membre de la famille, même si :
    - le service d'assistance technique le demande. Vous devez toujours saisir votre mot de passe vous-même pour ne pas le divulguer à l'employé du service d'assistance
    - vous vous absentez pour des vacances ou un congé
    - vous êtes remplacé temporairement
    - vous vous le faites demander par courriel.