Politique de mots de passe

Le 28 novembre 2023

Réseau FADOQ
7665, boulevard Lacordaire
Montréal (Québec) H1S 2A7

Téléphone : 514 252-3017
Sans frais : 1 800 544-9058
Télécopie : 514 252-3154
Courriel : info@fadoq.ca

Table des matières

Tableau des révisions

Niveau de révision	Date	Numéro de référence	Description sommaire de la révision	Auteur de la révision
Création	09-11-2023	Version 1	Pour approbation par le CA	Direction TI

Introduction

Une **politique de mots de passe** est une suite de règles destinées à améliorer la sécurité, en encourageant les utilisateurs à recourir à des mots de passe relativement robustes et en les utilisant correctement.

Objectifs

Le principal objectif est d'**augmenter la sécurité des accès** aux outils et informations diverses du Réseau FADOQ afin d'éviter ou de réduire les attaques informatiques visant à violer l'accès à nos données et usurper l'identité des utilisateurs.

Elle présente également l'avantage d'instaurer un cadre pour les utilisateurs, en vue d'appliquer une série de bonnes pratiques et de consignes à respecter pour la création et la gestion des mots de passe. La plupart des cyberattaques se produisent à partir de failles humaines.

Règles d'utilisation

- L'outil Dashlane est fourni à tous les employés du bureau. Dashlane est une **solution de gestion des mots de passe sécurisée**. Évitez d'utiliser d'autres gestionnaires de mots de passe pour les mots de passe d'entreprise, notamment en enregistrant les mots de passe dans votre navigateur Web.
- Lorsque c'est possible, utilisez le **générateur de mots de passe** de Dashlane pour créer des mots de passe uniques et complexes pour vos comptes professionnels. Lorsque ce n'est pas possible d'utiliser le générateur de mot de passe, veuillez utiliser un mot de passe fort (voir la section sur la création d'un mot de passe fort).
- N'utilisez pas un générateur de mot de passe pour le mot de passe de votre **compte Microsoft 365**. Vous devez pouvoir retenir celui-ci, car il est utilisé pour vous connecter à Dashlane et pour accéder à vos autres mots de passe. Le mot de passe pour votre compte Microsoft 365 doit être un mot de passe fort que vous devez retenir (voir la section sur la création d'un mot de passe fort).
- **Ne réutilisez pas vos mots de passe** personnels à des fins professionnelles ou le même mot de passe pour plusieurs comptes professionnels. Vous pouvez utiliser Dashlane pour identifier les mots de passe que vous réutilisez.
- Lorsque vous recevez un **nouveau mot de passe** pour un compte, lorsque c'est possible, modifiez-le à la suite à votre première connexion.
- **Partagez** en toute sécurité des mots de passe avec les autres employés en utilisant uniquement Dashlane.
- **Ne communiquez pas votre mot de passe** par téléphone, courriel ou messagerie instantanée.
- **Évitez de noter** vos mots de passe et de les **conserver** sur votre poste de travail.
- **Ajoutez l'authentification à 2 facteurs** à vos comptes les plus importants lorsque c'est possible. La mise en place de l'authentification à 2 facteurs pour les comptes Microsoft 365 est prévue prochainement.
- **Modifiez** votre mot de passe le plus rapidement possible si vous croyez qu'il a été **compromis**.

- N’enregistrez pas les mots de passe de vos **comptes personnels** dans le compte Dashlane **professionnel** fourni par la FADOQ. Dashlane offre un compte distinct gratuit de type « Friends & Family » qui peut être utilisé par les employés qui souhaitent utiliser le même outil pour leurs identifiants personnels. Pour ceux qui souhaitent utiliser cette offre, veuillez suivre la procédure fournie par le département informatique. Si vous n’êtes plus employé de la FADOQ, le compte personnel sera converti en compte de type « Gratuit » avec les limitations prévues par Dashlane pour ce type de compte. Vous devrez alors payer une licence Dashlane « Friends & Family » pour conserver les mêmes fonctionnalités. La FADOQ n’offre pas de support supplémentaire et se dégage de toute responsabilité relativement à l’utilisation de cette offre.

Création d’un mot de passe fort

Petit rappel

Lorsque c’est possible, il est conseillé d’utiliser le générateur de mots de passe de Dashlane pour créer des mots de passe uniques et complexes. Dashlane pourra ensuite les retenir pour vous. Cependant, n’utilisez pas un générateur de mot de passe pour le mot de passe de votre **compte Microsoft 365**. Vous devez pouvoir retenir celui-ci, car il est utilisé pour vous connecter à Dashlane et pour accéder à vos autres mots de passe.

Un mot de passe fort doit :

- Avoir au minimum 8 caractères (mais il est préférable d’en avoir au moins 12);
- Contenir au moins une minuscule et une majuscule;
- Contenir au moins un chiffre et un caractère spécial;
- Ne pas contenir d’informations personnelles faciles à trouver sur vous (sur les médias sociaux, par exemple : nom de votre animal de compagnie, date d’anniversaire, mets favori, etc.);
- Ne pas contenir de mots du dictionnaire, de noms propres, de séquences ou de répétitions de caractères (ex. : 1234, abcd);
- Être difficile à trouver.

Astuce pour créer un mot de passe fort

Vous pouvez utiliser la première lettre de chaque mot d’une phrase complète pour créer un mot de passe complexe plus facile à retenir.

Par exemple, la phrase « Le numéro de mon chandail de soccer est le 27! » pourrait donner le mot de passe « L#dmcdsel27! ». **Faire preuve de créativité !**