Directive sur la sécurité du mot de passe au Cégep

CÉGEP ÉDOUARD MONTPETIT

OBJECTIF :

Fournir aux utilisateurs les exigences relatives à la création et à la manière de gérer leurs mots de passe.

EXIGENCES SUR LE MOT DE PASSE :

La longueur minimale du mot de passe au Cégep est de 14 caractères. Le mot de passe doit être composé d'au moins 3 des 4 groupes suivants constitués d'au moins:

- Une lettre de l'alphabet minuscule;
- Une lettre de l'alphabet majuscule;
- Un chiffre compris entre 0 et 9;
- Un caractère spécial.

Les exigences supplémentaires

Le mot de passe **ne doit pas** :

- Correspondre à au moins 24 mots de passe précédents;
- Être facilement devinable;
- Être facilement accessible, il doit être codifié.

ACCEPTABILITÉ DU MOT DE PASSE :

Un mot de passe au Cégep est acceptable s'il atteint un score de 6 points. L'évaluation est basée sur la constitution de celui-ci.

Un mot interdit est un mot qui se trouve dans une base de données globale de mots interdits ou dans une base de données personnalisées de mots interdits (exemple: Édouard, Montpetit ...). Pour évaluer le score d'un mot de passe :

- Chaque mot interdit dans le mot de passe est noté à un point
- Chaque caractère isolé qui ne fait pas partir d'un mot interdit sera noté un point

La somme de ces points constitue le score de points pour un mot de passe.

> Exemple de mot de passe fort avec la longueur minimale requise : 1!2ed0u@rdec0le&A est un mot de passe acceptable avec un score de 7 (1, !, 2, ed0u@rd, ec0le, &, A) et qui contient deux mots interdits « Édouard » et « école ».

Date de mise à jour : 2023-03-08

CYCLE DE VIE DU MOT DE PASSE :

- Le mot de passe doit être changé dès la première connexion de l'utilisateur après la création de son compte au Cégep.
- L'ancien mot de passe ne doit en aucun cas être réutilisé.
- Les utilisateurs avec des privilèges doivent avoir un mot de passe complexe et robuste basé sur une phrase de passe.
- Le changement du mot de passe peut être forcé pour un utilisateur, pour qui il existe des preuves de compromission sur son compte.
- Le mot de passe de l'utilisateur doit être changé après la réactivation du compte de ce dernier et lorsque l'utilisateur quitte le Cégep.

LES ACTIONS SUR UN MOT DE PASSE : CHANGEMENT, RÉINITIALISATION OU VERROUILLAGE :

- Dans le cas où l'utilisateur souhaite changer son mot de passe, ce changement doit se faire par le système libre-service du Cégep.

Pour l'accès au système libre-service, via le lien suivant :
https://motdepasse.cegepmontpetit.ca

Le centre de service informatique doit orienter l'usager en priorité vers ce moyen. Dans un cas exceptionnel où l'utilisateur ne peut pas le faire par ce système, le centre de service fera le changement et communiquera le nouveau mot de passe temporaire à l'usager qui le changera à la prochaine connexion.

- Les mots de passe par défaut des comptes d'accès aux applications ou équipements qui sont ajoutés par des éditeurs ou des constructeurs doivent être modifiés.
- Lorsqu'un évènement se produit en mode libre-service, l'utilisateur est notifié par courriel.
- Les administrateurs généraux doivent être notifiés, lorsqu'un administrateur privilégié réinitialise son mot de passe en libre-service.
- L'utilisateur doit recevoir un courriel de notification lorsque son mot de passe est modifié.
- Le compte de l'usager est verrouillé lorsque plusieurs tentatives de connexion avec un mot de passe erroné ont échoué.

Date de mise à jour : 2023-03-08

LES PRATIQUES À ADOPTER

Pour assurer une sécurité supplémentaire au mot de passe :

- Il ne doit pas être formé d'un mot que l'on peut trouver dans un dictionnaire ou contenir les informations personnelles comme la date de naissance, le nom d'une personne, le nom d'un produit, etc.
- Il doit être facile à mémoriser et ne doit pas être inscrit dans un fichier ou sur un support (papier, pense-bête, etc.).
- Il faut avoir un mot de passe fort basé sur une phrase secrète dont vous vous souviendrez facilement.
- Avant de fournir votre mot de passe sur un lien fourni par le Cégep, assurez-vous que ce lien est sécurisé. L'URL doit toujours commencer par https:// et non http://, même si vous êtes dans l'un de nos campus.
- Ne tapez pas votre mot de passe pendant qu'une personne regarde. Changer rapidement votre mot de passe lorsque vous jugez que celui-ci est vu par une personne lors de votre saisie au clavier, et ce peu importe par qui.
- Le mot de passe ne doit pas être partagé avec une autre personne, même si ce dernier est un membre de l'équipe informatique.
- Ne fournissez pas votre mot de passe par courriel, Microsoft Teams, au téléphone ou tout autre moyen de communication à un tiers, même pas votre supérieur.
- Avoir un coffre-fort de mots de passe qui permet de générer une série de caractères complexes et qui permet de stocker les mots de passe de manière sécurisée.
- Ne pas utiliser le gestionnaire de mots de passe proposé par un navigateur Internet.
- N'utilisez jamais vos mots de passe du Cégep à des fins non professionnelles.

CHAMP D'APPLICATION :

Cette directive s'applique pour tous les mots de passe des comptes :

- Toutes les ressources du réseau local.
- Toutes les ressources infonuagiques.
- Omnivox, Clara, Mia pour les étudiants et les enseignants.
- Autres équipements et services essentiels.

Date de mise à jour : 2023-03-08