Norme relative aux mots de passe

1.1 Aperçu

Les mots de passe constituent un fondement essentiel de la sécurité informatique. Ils représentent la première ligne de protection des comptes utilisateur. Des mots de passe mal conçus peuvent affaiblir le degré de sécurité des technologies de l'information du Partenariat.

Afin de veiller à ce que les ressources informationnelles et de technologies de l'information (TI) du Partenariat demeurent, en tout temps, sécurisées comme il se doit, le présent document définit des contrôles efficaces en matière de mot de passe. Le Partenariat pourrait, à sa seule discrétion, imposer des directives supplémentaires en la matière.

1.2 But

Ce document a pour but de fournir un ensemble de normes minimales en matière de sécurité et de protection des renseignements personnels (ci-après appelé « la norme ») à mettre en œuvre dans le cadre de la sécurisation des ressources informationnelles et TI du Partenariat grâce à l'utilisation de mots de passe.

1.3 Portée

Cette norme s'applique à l'ensemble du personnel, des consultants et des sous-traitants du Partenariat qui utilisent ses ressources TI. **Elle ne s'applique ni au système téléphonique Cisco ni aux imprimantes multifonctions Ricoh du Partenariat.**

1.4 Normes

i. Tous les mots de passe des utilisateurs expireront après 90 jours.
ii. Les utilisateurs ne pourront réutiliser les dix mots de passe précédents associés à leur compte utilisateur.
iii. Les utilisateurs pourvus de comptes utilisateur dotés de privilèges de niveau « système » octroyés en vue de l'accès à certaines ressources informationnelles et TI du Partenariat

devront utiliser, pour le stockage sécuritaire des mots de passe de ces comptes « administrateur », le logiciel fourni par le Partenariat à cet effet.

iv. Les mots de passe ne devront être insérés ni dans des courriels ni dans d'autres formes de communication électronique.

v. Tous les mots de passe devront avoir une longueur minimale de huit caractères et être conformes aux directives décrites ci-dessous.

vi. L'utilisation de mots de passe difficiles à deviner constitue un fondement essentiel de la sécurité des systèmes. La meilleure façon de créer des mots de passe robustes consiste à utiliser les initiales d'une phrase secrète comportant plus de 15 caractères. Tous les mots de passe ou toutes les phrases secrètes devront comporter les caractéristiques ci-après.

- Ils devront obligatoirement contenir des caractères appartenant à chacune des quatre catégories suivantes :
  - Caractères alphabétiques en majuscules (A à Z)
  - Caractères alphabétiques en minuscules (a à z)
  - Caractères numériques (0 à 9)
  - Caractères non alphanumériques « spéciaux » (par exemple #$^%!+?/).
- Ils ne devront pas être basés sur des renseignements personnels, par exemple le nom d'un membre de la famille.
- Ils ne devront être ni écrits sur un papier ni stockés en ligne, sauf si des mesures spécifiques ont été mises en place pour les protéger d'un accès non autorisé.

vii. Ils devront être traités en respectant des règles de stricte confidentialité.

viii. Les mots de passe ne devront être transmis à aucune autre personne, à l'exception du centre de services informatiques du Partenariat dans des situations de résolution de problèmes ou de maintenance.

ix. Si un tiers prend connaissance d'un mot de passe, ce dernier devra être réinitialisé immédiatement.

x. Dans certains cas, une authentification est requise pour l'accès aux ressources informationnelles et TI du Partenariat depuis l'extérieur de ses locaux. Les circonstances dans lesquelles une authentification est requise et le type d'authentification requis dans chaque cas sont décrits dans la Politique de sécurité de l'information et des technologies de l'information.

1.5 Contrôle de l'application de la politique

En cas de non-respect de cette norme, le Partenariat pourra, sans que cela soit limitatif, prendre les mesures suivantes :

i. Refuser l'accès à ses ressources informationnelles et TI.
ii. Mettre en œuvre, pour les fournisseurs indépendants, les consultants ou les sous-traitants, les recours contractuels appropriés, par exemple les dispositions relatives aux manquements au contrat ou à sa résiliation.
iii. Mettre en œuvre, pour le personnel, des mesures disciplinaires pouvant inclure, sans que cela soit limitatif, un avertissement écrit, une suspension avec ou sans traitement ou un licenciement immédiat motivé sans aucun préavis ni autre obligation.

1.6 Définitions

Terme	Définition
Ressources informationnelles et TI	Matériel informatique (y compris les ordinateurs portatifs et de bureau), logiciels, systèmes d'exploitation, supports de stockage, comptes réseau, courrier électronique, accès Internet, portails, passerelles, appareils réseau, appareils mobiles, serveurs, téléphones et systèmes téléphoniques, imprimantes multifonctions, ordinateurs personnels et domestiques connectés au réseau du Partenariat, directement ou par l'entremise d'une connexion VPN, ressources informationnelles (quel que soit le support ou le format), par exemple les renseignements commerciaux ou personnels, ainsi que tout autre élément que le Partenariat pourrait considérer comme une ressource informationnelle ou TI
Utilisateur	Toute personne qui consulte et utilise les ressources informationnelles et TI du Partenariat

1.7 Documents connexes

- Politique de sécurité de l'information et des technologies de l'information
- Politique d'utilisation acceptable
- Politique sur les appareils mobiles
- Politique « Apportez votre équipement personnel de communication » (AVEC)
- Norme relative au courrier électronique

Fin du document