Directive du Bureau du Chef de l'Information : TI 8.03	Publié : 04/2019
Chapitre : Sécurité physique et sécurité des systèmes	Dernière révision : 01/2024
Objet : **IDENTIFICATION et MOTS DE PASSE DES UTILISATEURS**	

1 DIRECTIVE

1.1 L'accès à un système informatique hôte, à un serveur de réseau ou à un appareil informatique en réseau fourni par le GNB doit être approuvé par le gestionnaire de l'utilisateur, qui doit transmettre une demande d'accès au Bureau des services de la TI (par l'intermédiaire de la personne désignée sur le tableau des autorités).

L'organisation contrôlera l'accès aux systèmes d'information et aux données, y compris à tout ordinateur hôte, serveur de réseau, ordinateur personnel en réseau et appareil mobile, en mettant en œuvre des politiques et des procédures rigoureuses d'authentification des utilisateurs et de gestion des mots de passe pour les services sur place ou en nuage.

2 OBJECTIF

2.1 L'objectif de la présente directive est de s'assurer :

- que l'approbation par la direction de l'accès au système accordé à chaque personne est inscrite au dossier;
- que seul le personnel autorisé à accéder au système informatique, au réseau ou aux serveurs y a accès;
- que toutes les activités sur le système, le réseau ou les serveurs peuvent être associées à une personne;
- que les mots de passe pour l'authentification des utilisateurs sont conservés en sécurité;
- qu'une personne peut être tenue responsable de toutes les activités effectuées sous son identifiant.

3 PORTÉE

3.1 La présente directive s'applique à tous les employés qui ont accès au système.

4 RESPONSABILITÉ

4.1 Chaque gestionnaire est responsable d'évaluer les besoins d'accès aux systèmes de ses employés et d'approuver l'accès des employés qui en ont besoin pour exercer leurs fonctions.

4.2 Les **Opérations de la TI** doivent :

a) tenir à jour les renseignements sur les identifiants des utilisateurs et conserver dans les fichiers les demandes signées d'accès aux systèmes;

b) fournir aux utilisateurs un identifiant et un mot de passe expiré

pour la première connexion;

c) remplacer le mot de passe par un nouveau mot de passe expiré si un utilisateur demande de l'aide parce qu'il soupçonne que son mot de passe pourrait être compromis ou parce qu'il a oublié son mot de passe;

d) créer et maintenir un système d'administration de l'identification des utilisateurs et de leurs mots de passe;

e) comprendre les risques associés à l'identification des utilisateurs et aux mots de passe;

f) concevoir et mettre en œuvre des politiques de mot de passe rigoureuses selon les pratiques exemplaires actuelles;

g) réduire le recours aux mots de passe dans la mesure du possible;

h) réduire le fardeau des utilisateurs pour atténuer la surcharge de mots de passe;

i) mettre en œuvre des solutions technologiques ou automatisées dans les systèmes d'identification des utilisateurs et de gestion des mots de passe lorsque cela est possible;

j) aider les utilisateurs à créer des mots de passe forts;

k) accompagner et former les utilisateurs.

4.3 L'utilisateur doit :

a) assurer la confidentialité de son mot de passe. Il est interdit de communiquer son mot de passe;

b) modifier son mot de passe à la première connexion et régulièrement par la suite selon la classification des données auxquelles il a accès;

c) respecter les directives pour la création d'un mot de passe pour assurer la confidentialité de son mot de passe;

d) informer le **Bureau des services de la TI** de tout soupçon de communication d'un mot de passe ou d'utilisation malveillante de l'identifiant d'un utilisateur.

Remarque : L'utilisateur est également responsable de toute activité de traitement associée à son identifiant.

5 DÉFINITIONS

Identifiant de l'utilisateur désigne une combinaison unique de caractères qui permet de reconnaître un utilisateur lorsqu'il accède à un système.

6 DIRECTIVES CONNEXES

BCI TI 6.02 – Administration de l'accès
BCI TI 7.02 – Contrôles de la journalisation
BCI TI 8.02 – Sécurité des systèmes
BCI TI 9.06 – Cryptage des données
BCI TI 13.01 – Accès aux systèmes et utilisation acceptable des systèmes
BCI TI 13.02 – Accès aux données et protection des données
BCI TI 13.03 – Mots de passe