Directive du Bureau du Chef de l'Information : TI 13.09	Publié : 04/2019
Chapitre : Responsabilités des utilisateurs	Dernière révision : 01/2024
Objet : Accès à distance – utilisateurs	

1 DIRECTIVE

1.01 Les utilisateurs qui ont besoin d'un accès à distance doivent obtenir l'autorisation de la direction pour se connecter aux installations informatiques de l'organisation à partir d'un site extérieur.

1.02 Les utilisateurs ayant la capacité de se connecter à distance aux installations informatiques de la Politique de sécurité de l'information du GNB :

a) Doivent suivre les directives de sécurité fournies par le service de soutien technique de la TI en ce qui concerne l'accès à leurs dispositifs informatiques, la configuration de leur logiciel de connexion à distance et la maintenance de leur système d'exploitation.

b) Ne doivent pas utiliser des comptes de courrier électronique autres que ceux de l'organisation, tels que Hotmail, Yahoo ou AOL pour s'occuper des affaires de l'organisation.

c) Doivent respecter les mêmes restrictions concernant l'utilisation des installations et des ressources de l'organisation lorsqu'elles sont connectées à distance qui sont définies dans toutes les politiques sur les responsabilités de l'utilisateur pour une utilisation sur place.

d) Ne doivent pas désactiver ou contourner les mesures de sécurité imposées par l'organisation, telles que les logiciels antivirus ou les limites d'inactivité et les actions automatisées connexes.

e) Doivent maintenir leurs systèmes à distance en utilisant tous les correctifs de sécurité disponibles en temps opportun.

f) Doivent tenir à jour les définitions et les logiciels antivirus.

g) Ne peuvent activer la capacité de connexion sans fil sur un ordinateur client ou portable connecté au réseau qu'avec l'autorisation écrite du service de soutien technique de la TI.

h) Ne doivent pas divulguer à une personne non autorisée les paramètres de configuration à distance qui permettent de se connecter à distance aux installations informatiques de la Politique de sécurité de l'information du GNB.

2 OBJET

2.01 La présente directive a pour objet de faire en sorte que :

a) Les utilisateurs qui ont une capacité d'accès à distance approuvée disposent de moyens sécurisés pour accéder aux systèmes d'information de la Politique de sécurité de l'information du GNB;

b) Les systèmes, les réseaux et les données de l'organisation sont protégés adéquatement contre les menaces de sécurité provenant de systèmes informatiques gérés hors des locaux et du contrôle de la Politique de sécurité de l'information du GNB;

c) Seuls les utilisateurs autorisés ayant reçu une formation appropriée sur

les procédures d'accès à distance sécuritaires peuvent se connecter aux systèmes et réseaux de l'organisation au moyen de connexions à distance.

3 PORTÉE

3.01 La présente directive s'applique à tous les utilisateurs autorisés à accéder à distance aux ressources informatiques de l'organisation.

4 RESPONSABILITÉ

4.01 Le **service de soutien technique de la TI** est responsable de fournir aux utilisateurs de connexions à distance des renseignements qui leur permettent de comprendre l'importance de la sécurité de leurs réseaux domestiques et de leurs ordinateurs portatifs et les méthodes courantes pour les sécuriser.

4.02 Les utilisateurs d'accès à distance doivent :

a) Avoir l'approbation consignée de la direction et une justification opérationnelle pour se connecter à partir d'un emplacement hors site;

b) Limiter leur accès à distance aux appareils et réseaux informatiques approuvés par le service de soutien technique de la TI;

c) Limiter l'accès à distance de leurs appareils informatiques aux utilisateurs approuvés par la direction (pas de famille, d'amis, de visiteurs ou d'intrus);

d) Configurer et maintenir des dispositifs informatiques qui accèdent aux ressources informatiques de l'organisation à distance, conformément à l'énoncé de la directive ci-dessus;

e) Protéger leurs mécanismes d'accès à distance (identité, mots de passe, appareils, etc.) contre toute utilisation non autorisée ou perte;

f) Conserver les appareils personnels ayant une capacité d'accès à distance dans des lieux sécurisés;

g) S'abstenir de se connecter au site de la Politique de sécurité de l'information du GNB tout en étant simultanément connecté à tout autre réseau, à l'exception d'un réseau personnel qu'ils contrôlent entièrement;

h) S'abstenir de contourner tout mécanisme de sécurité requis par le service de soutien technique de la TI, comme les délais d'inactivité et les interventions sur le système de l'utilisateur ou sur le site de la Politique de sécurité de l'information du GNB (p. ex. 30 minutes sans activité du clavier ou de la souris, reconnexion et connexion automatiques, utilitaire PING pour simuler une connexion au réseau qui n'est pas au ralenti).

5 DÉFINITIONS

5.01 « **RPV** » (**réseau privé virtuel**) désigne la configuration d'un canal de communication sécurisé et crypté par le biais d'un réseau public tel que

l'Internet.

6 DIRECTIVES CONNEXES

BCI TI 10.03 – Accès à distance
BCI TI 10.04 – Réseau sans fil
BCI TI 10.08 – Messagerie instantanée
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 – Sélection et contrôle
BCI TI 13.06 – Écran effacé et verrouillé
BCI TI 13.07 – Supports amovibles
BCI TI 13.08 – Ordinateurs portables
BCI TI 14.01 – AVEC : Dispositifs et systèmes d'exploitation acceptables
BCI TI 14.02 – AVEC : Accès aux systèmes et utilisation acceptable des systèmes