1 DIRECTIVE

1.01 La connectivité aux réseaux sans fil doit être mise en œuvre en utilisant les précautions et les paramètres de configuration les plus efficaces de l'industrie sur le plan de la sécurité.

1.02 Quand la connectivité aux réseaux sans fil est mise en œuvre, Planification du réseau et Soutien de la TI doivent réévaluer les risques pour la sécurité au moins une fois par trimestre en ce qui a trait aux expositions connues aux risques. Cette évaluation pourra entraîner :

a) la suspension du soutien de la connectivité sans fil jusqu'à ce qu'on puisse diminuer les risques;

b) l'imposition d'autres restrictions à la connectivité sans fil;

c) la mise en œuvre de nouveau matériel ou de nouveaux logiciels pour réduire ou pour éliminer les nouveaux risques.

1.03 Les utilisateurs qui emploient des appareils qui permettent la connectivité sans fil au réseau du GNB doivent observer toutes les règles visant à empêcher les accès non autorisés au réseau, à empêcher l'utilisation non autorisée de ces appareils eux-mêmes et se conformer à l'utilisation obligatoire des mots de passe et du matériel d'authentification.

2 OBJET

2.01 La présente directive a pour objet d'assurer que la connectivité sans fil au réseau du GNB n'augmente pas indûment le risque de perte ou de dommages pour les ressources de la TI et les données du GNB.

3 PORTÉE

3.01 La présente directive s'applique à Planification du réseau, à Soutien de la TI et à tous les utilisateurs d'appareils sans fil qui permettent la connectivité au réseau.

4 RESPONSABILITÉ

4.01 Planification du réseau a les responsabilités suivantes :

a) concevoir des modalités d'accès au réseau qui minimisent les risques pour la sécurité;

b) se tenir au courant des toutes dernières menaces pour les réseaux sans fil;

c) planifier des mises à niveau pour protéger les réseaux du GNB contre les nouvelles menaces.

4.02 Soutien de la TI a les responsabilités suivantes :

a) configurer le matériel sans fil pour éliminer ou minimiser les risques;

b) se tenir au courant des toutes dernières menaces pour les réseaux sans fil;

c) gérer les risques pour le réseau sans fil au besoin, y compris en suspendant le service sans fil quand des menaces sont découvertes pour la sécurité.

4.03 Les utilisateurs d'appareils configurés pour la connectivité sans fil sont tenus de suivre les directives de Soutien de la TI pour minimiser les risques pour la sécurité quand la connectivité au réseau est activée dans leurs appareils sans fil.

5 DÉFINITIONS

5.01 **« 802.11 »** est un ensemble de spécifications pour les réseaux sans fil locaux, élaborées par un groupe de travail de l'Electrical and Electronics Engineers (IEEE). Cet ensemble compte plusieurs spécifications, dont 802.11a, 802.11b, 802.11g et 802.11i. D'autres spécifications sont attendues en réponse à l'évolution constante de la performance ou de la sécurité.

5.02 L'**« AES** » (**Advanced Encryption Standard/Norme de chiffrement avancé**) est une technique de chiffrement des données qui utilise un bloc de 128 bits, mise au point par les cryptographes belges John Daemon et Vincent Rijmen, qui a remplacé l'algorithme de chiffrement DES employé par le gouvernement américain jusqu'en octobre 2000.

6 DIRECTIVES CONNEXES

BCI TI 9.06 – Cryptage des données

BCI TI 10.01 – Connexion au réseau par matériel externe

BCI TI 10.02 – Protection pare-feu

BCI TI 10.03 – Accès à distance

BCI TI 10.08 – Messagerie instantanée

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 13.09 – Accès à distance – Utilisateurs