Directive du Bureau du Chef de l'Information: TI 5.07	Publié: 02/2020
Chapitre: Gestion des données	Dernière révision: 01/2022
Objet: **Exigences anti-pourriel**	

1 DIRECTIVE

1.01 La Politique de protection de l'information du GNB sera conforme à la *Loi canadienne anti-pourriel* (communément appelée « LCAP »).

1.02 La haute direction s'assurera que les politiques, les procédures, les pratiques et les bases de données de l'organisation sont établies et conformes à la LCAP.

2 OBJET

2.01 La présente directive a pour objet d'assurer la conformité de la politique de protection de l'information du GNB avec la LCAP, d'éviter des sanctions réglementaires et des poursuites ainsi que de protéger l'image de marque du GNB pour les activités suivantes :

1. envoi de messages électroniques commerciaux (MEC);
2. **modification des données de transmission** pour remettre les données à une destination différente de celle voulue par l'expéditeur;
3. **installation de programmes d'ordinateur (c.-à-d. des logiciels)** dans les systèmes informatiques de tiers;
4. **collecte d'adresses électroniques sans consentement** (c.-à-d. recueil d'adresses électroniques en utilisant des logiciels conçus précisément à cette fin ou utiliser des adresses électroniques collectées de cette manière).

3 PORTÉE

3.01 La présente directive s'applique à tous les employés, entrepreneurs indépendants, fournisseurs de services externes et partenaires opérationnels (c.-à-d. le personnel) qui exécutent n'importe laquelle des activités ci-dessus, pour l'organisation ou en son nom.

3.02 La présente directive s'applique aux activités ayant un lien avec le Canada, ce qui signifie un système informatique situé au Canada qui est utilisé pour envoyer le MEC ou y accéder; ou pour expédier, acheminer les données transmises par voie électronique qui ont été modifiées ou pour accéder à celles-ci. Pour les installations de logiciel, au moment où la contravention est commise, le système informatique doit être au Canada ou les installateurs ou les personnes qui dirigent l'installation doivent être au Canada au moment où ils donnent ces instructions. Par conséquent, la LACP s'applique aux partenaires opérationnels internationaux agissant au nom de l'organisation au Canada ou interagissant avec les clients canadiens.

3.03 La présente directive s'applique également aux personnes indirectement responsables d'infractions à la LCAP. Donc, des termes comme « expédier », « installer », « modifier » ou des termes similaires employés dans la présente

directive peuvent s'appliquer à ceux qui sont à l'origine de l'activité en question.

4 RESPONSABILITÉ

4.01 La haute direction est responsable de la surveillance des modifications de la loi et des pratiques exemplaires ainsi que de la mise à jour régulière de la présente directive.

4.02 La haute direction est responsable de la conduite des vérifications de la conformité à la LCAP et des enquêtes concernant le non-respect de la LCAP ou de la présente directive ou des plaintes à ce sujet.

4.03 La haute direction et tous les autres chefs de service sont responsables de la supervision de leurs subordonnés directs et des fonctions ministérielles pour assurer la conformité à la LCAP et à la présente directive et doivent aviser le chef de la sécurité de l'information des infractions, des plaintes ou des sujets de préoccupation relatifs à la LCAP ou à la présente directive.

4.04 Tous les membres du personnel sont responsables de respecter la LCAP et la présente directive. Les infractions à la présente directive peuvent donner lieu à des mesures disciplinaires pouvant aller jusqu'au congédiement.

5 DÉFINITIONS

5.01 **LCAP** (voir la section 6 ci-dessous).

5.02 Un **MEC** (**message électronique commercial**) est un message électronique qui encourage la participation à une activité commerciale.

Les messages électroniques qui comportent une demande de consentement en vue de la transmission de MEC sont des MEC eux-mêmes.

Les conversations téléphoniques, les messages envoyés par télécopieur et les messages téléphoniques ne sont pas des MEC, mais ils peuvent être réglementés par la voie du « registre des abonnés auto-exclus ». Les messages électroniques envoyés à des fins d'observation de la loi, de sécurité publique et de sécurité nationale ou internationale ne sont pas non plus des MEC.

5.03 Une **activité commerciale** est toute activité de nature commerciale, y compris les activités qui ne sont pas accomplies dans le but de réaliser un profit. Les activités suivantes sont des exemples d'activités commerciales : une offre de

vente, de louage ou de troc d'un produit, ou d'un service et la promotion d'une possibilité d'affaires, de jeu ou d'investissement. Les activités d'application de la loi ou liées à la sécurité publique ne sont pas des activités commerciales.

5.04 Les **systèmes informatiques** sont les ordinateurs, les ordinateurs portables, les tablettes, les consoles de jeux, les téléphones intelligents ou les autres appareils connectés.

5.05 Un **message électronique** est un message envoyé par télécommunication, notamment les messages textes, le service de messages courts (c.-à-d. la messagerie instantanée, comme BlackBerry Messenger [BBM] ou WhatsApp) et les messages des médias sociaux.

5.06 Les **données de transmission** sont souvent appelées métadonnées, soit les données sous-jacentes qui donnent de l'information sur d'autres données. Les métadonnées font partie des messages électroniques pour faciliter des fonctions de télécommunication comme la signalisation, la connexion, la composition, le routage et l'adressage ou elles sont produites pendant les télécommunications.

« L'hameçonnage » et le « détournement de connexion » sont des exemples d'escroqueries à base de **modification de données de transmission** non autorisée. Les « hameçonneurs » envoient des courriels soi-disant légitimes qui demandent à leurs destinataires d'ouvrir une session en utilisant un lien fourni et d'effectuer des transactions bancaires, par exemple. Le lien les dirige en réalité vers un site frauduleux où leurs informations de connexion et leurs renseignements personnels sont volés, puis utilisés pour les escroquer. Le « détournement de connexion » emploie des moyens techniques pour réacheminer des personnes vers des sites Web frauduleux afin d'obtenir des résultats comparables.

5.07 L'**utilisateur** désigne le propriétaire ou l'utilisateur autorisé d'un système informatique. Un utilisateur autorisé est toute personne ayant reçu la permission d'utiliser le système informatisé. Par exemple : (i) un organisme employeur est le propriétaire de son système informatique; ses employés, administrateurs ou dirigeants en sont les utilisateurs autorisés; (ii) les parents sont les propriétaires des systèmes informatiques et leurs enfants en sont les utilisateurs autorisés.

6 DIRECTIVES CONNEXES

6.01 La Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique et modifiant la *Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes*, la

Loi sur la concurrence, la *Loi sur la protection des renseignements personnels* et les *documents électroniques,* la *Loi sur les télécommunications* (L.C. 2010, ch. 23) et La *Loi sur les télécommunications* (L.C. 2010, ch. 23) et la réglementation connexe (p. ex. LCAP).

BCI TI 5.02 – Sauvegarde et stockage de données

BCI TI 5.04 – Gestion de bases de données

BCI TI 8.04 – Confidentialité et protection des renseignements personnels