Directive du Bureau du Chef de l'Information : TI 8.06	Publié : 04/2019
Chapitre : Sécurité physique et sécurité des systèmes	Dernière révision : 01/2024
Objet : **GESTION d'une ATTEINTE À LA SÉCURITÉ**	

1 DIRECTIVE

1.01 La **politique de protection de l'information du GNB** comprendra toutes les mesures raisonnables pour assurer la confidentialité des renseignements personnels sous le contrôle du GNB par l'élaboration et la mise en œuvre de politiques et procédures se penchant sur les **atteintes aux mesures de sécurité (c.-à-d. atteinte à la sécurité)**.

2 OBJET

2.01 La présente directive a pour **objet** de décrire l'intervention de GNB en cas d'atteinte à la sécurité.

3 PORTÉE

3.01 La présente directive s'applique au conseil d'administration, à tous les employés, de même qu'aux **fournisseurs** et consultants qui fournissent des biens et services au GNB (c.-à-d. au personnel du GNB), et elle s'applique dans tous les cas d'atteinte à la sécurité avérée ou soupçonnée.

4 RESPONSABILITÉ

4.01 Le **sous-ministre du Conseil du Trésor** et le **chef du service de l'information, de pair avec d'autres membres de la haute direction**, s'assureront que la direction élabore, tient à jour et met à l'essai les politiques, directives et procédures qui conviennent pour gérer les atteintes à la sécurité, afin d'assurer le respect des lois et pratiques exemplaires applicables.

4.02 Tous les employés du **GNB** sont responsables de respecter les mesures de sécurité établies. Si une mesure de sécurité requise n'a pas encore été mise en œuvre, le personnel du GNB doit opter pour un plan d'action qui réduira au minimum la probabilité d'une atteinte à la sécurité et les répercussions potentielles.

4.03 Le **sous-ministre du Conseil du Trésor** formera une **équipe d'intervention en cas d'atteinte à la sécurité (EIAS)**, laquelle devrait être dirigée par le **chef de la sécurité de l'information (CSI)** et le **chef de la protection des renseignements personnels (CPRP)**. L'**EIAS** doit aussi compter des représentants de différentes unités fonctionnelles, dont la technologie de l'information (TI), les ressources humaines, les finances, les relations publiques et communications, la gestion du risque et les services juridiques. Les participants externes peuvent comprendre un consultant externe, des experts en TI, des représentants en assurance du GNB et des entreprises de relations publiques.

4.04 Le **chef de la sécurité de l'information (CSI)** et le **chef de la protection des renseignements personnels (CPRP)** sont responsables de mobiliser et de diriger les protocoles en cas d'atteinte à la sécurité lorsqu'ils sont informés d'une atteinte avérée ou soupçonnée à la sécurité.

4.05 L'**EIAS** aidera le CSI et le CPRP à mobiliser les protocoles en cas d'atteinte à la sécurité. La présente directive attribue des responsabilités au CSI et au CPRP, mais ces derniers peuvent déléguer l'exécution de ces tâches à d'autres membres de l'**EIAS** tout en demeurant responsables des tâches déléguées.

5 DÉFINITIONS

5.01 **Atteinte aux mesures de sécurité (c.-à-d. atteinte à la sécurité)** désigne la perte ou la communication de renseignements personnels ou l'accès non autorisé à ceux-ci découlant d'une atteinte aux mesures de sécurité du GNB ou du défaut du GNB à mettre en place de pareilles mesures.

5.02 **Renseignement personnel** s'entend d'un renseignement qui peut être directement ou indirectement associé à une personne en particulier, par référence à un numéro d'identification ou à un ou plusieurs éléments propres à son identité physique, psychologique, économique, culturelle ou sociale. Les renseignements personnels comprennent ce qui suit :

- Nom, numéros d'identification
- Dossiers, évaluations, commentaires, mesures disciplinaires, revenu, profil salarial des employés
- Dossiers de crédit, registres de prêt, existence d'un conflit entre un consommateur et un marchand
- Renseignements médicaux ou renseignements sur la santé, groupe sanguin
- Origine ethnique, croyances religieuses ou philosophiques, opinions politiques

Les renseignements personnels peuvent aussi comprendre les coordonnées professionnelles, comme le numéro de téléphone ou l'adresse courriel au travail, s'ils sont utilisés pour une fin autre que communiquer avec la personne en lien avec son emploi, son entreprise ou sa profession.

5.03 **Risque réel de préjudice grave** s'entend d'un risque réel ou de la probabilité qu'un préjudice grave survienne en raison de la sensibilité des renseignements personnels en cause, de la probabilité que les renseignements aient été mal utilisés ou de tout autre facteur réglementaire associé aux renseignements

compromis. Un préjudice grave vise notamment la lésion corporelle, l'humiliation, le dommage à la réputation ou aux relations, la perte financière, le vol d'identité, l'effet négatif sur le dossier de crédit, le dommage aux biens ou leur perte, et la perte de possibilités d'emploi ou d'occasions d'affaires ou d'activités professionnelles.

6 DIRECTIVES CONNEXES

Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE), lois provinciales applicables sur la protection des renseignements personnels

Loi sur la protection des renseignements personnels numériques

BCI TI 4.02 – Gestion des accès et des rôles d'utilisateurs

BCI TI 4.03 – Accès à l'Internet

BCI TI 6.02 – Administration de l'accès

BCI TI 9.03 – Contrôles de l'accès aux données

BCI TI 8.04 – Confidentialité et protection des renseignements personnels