Directive du Bureau du Chef de l'Information : TI 9.03	Diffusion : 2020-02
Chapitre : Sécurité des données	Dernière révision : 01/2022
Objet : **Mesures de contrôle de l'accès aux données**	

1 DIRECTIVE

1.01 Des mesures de contrôle de l'accès doivent être établies dans le cas de toutes les données classifiées à titre de données **« confidentielles »** ou d'un niveau supérieur.

2 OBJET

2.01 La présente directive vise à assurer la mise en place de mesures de contrôle adéquates de l'accès aux données en fonction de la classification des données.

3 PORTÉE

3.01 La présente directive s'applique à tous les employés.

4 RESPONSABILITÉ

4.01 Les responsables opérationnels doivent :

a) restreindre l'accès à leurs données classifiées à titre de données **« confidentielles »** ou d'un niveau supérieur. Si l'accès aux données est délégué à un groupe opérationnel, les responsables doivent communiquer les mesures de contrôle de la classification des données requises au groupe opérationnel;

b) gérer, tenir à jour et revoir les listes d'approbation de l'accès à leurs données classifiées à titre de données **« confidentielles »** ou d'un niveau supérieur;

c) vérifier les registres d'accès aux données classifiées à titre de données « hautement confidentielles »;

d) s'assurer que des mesures de contrôle suffisantes sont accessibles dans tous les systèmes permettant un accès en mode lecture à leurs données classifiées à titre de données **« confidentielles »** ou d'un niveau supérieur;

e) mettre à jour les listes d'accès lorsqu'ils sont avisés du départ d'un employé de l'organisation.

4.02 Les administrateurs des systèmes de TI ont la responsabilité de :

a) gérer les mesures de contrôle de l'accès aux données suivant les directives des responsables opérationnels;

b) déterminer le niveau le plus élevé de classification des données que peut gérer leur système.

4.03 Les utilisateurs qui ont accès aux données classifiées à des niveaux supérieurs

au niveau « public » ont la responsabilité de respecter les mesures de contrôle requises pour l'accès aux données correspondant à la classification des données. Si un utilisateur copie des données classifiées à un niveau supérieur au niveau « public », il doit contrôler l'accès à la copie correspondant à leur classification.

Les utilisateurs ne peuvent copier en aucun cas des données classifiées à titre de données « hautement confidentielles ».

5 DÉFINITIONS

5.01 Le **« responsable opérationnel »** est un cadre supérieur de l'organisation qui est responsable de la gestion générale d'une application ou d'un secteur d'activité. Il a le pouvoir de déterminer qui peut accéder aux données et les utiliser, et il bénéficie habituellement du soutien des gestionnaires de données. Le responsable opérationnel approuve les processus et les politiques visant à maintenir la qualité des données et à normaliser les processus de gestion des données.

5.02 Les employés affectés à des contrats/documents gouvernementaux de nature délicate pourraient avoir besoin d'une **cote de fiabilité (CF)** pour accéder aux biens et renseignements confidentiels.

5.03 Cote de sécurité personnelle (CSP)

Les employés affectés à des contrats gouvernementaux de nature délicate doivent avoir une telle cote pour accéder aux renseignements classifiés à un niveau supérieur au niveau hautement confidentiel du GNB ou au niveau Protégé C du gouvernement fédéral (cela englobe les normes fédérales *confidentiel*, *secret* et *très secret*). Cette cote est utilisée pour les transferts au gouvernement fédéral.

5.04 Niveaux de classification de cybersécurité

Les niveaux de classification des données sont définis en fonction du niveau de contrôle auquel doit être assujettie la communication des données à l'intérieur de l'organisation compte tenu des pertes ou des préjudices que pourrait subir l'organisation en cas de divulgation accidentelle ou malveillante au public ou à la concurrence. Différents types de classification sont prévus, notamment :

Les données **« publiques »** désignent les données pouvant être communiquées à l'extérieur de l'organisation. La communication publique de ces données pourrait être préalablement approuvée parce qu'elle est

souhaitable ou parce que les données doivent être du domaine public. Mentionnons par exemple les rapports annuels, la divulgation publique des profits, les nouvelles et les annonces.

Les données **« internes »** sont des données opérationnelles du GNB qui ne sont toutefois pas publiques. Cette catégorie s'applique aux fonds de renseignements qui pourraient causer un préjudice à une personne, à une organisation ou à un gouvernement s'ils étaient compromis.

Exemples : rapports préliminaires avant leur publication, analyses et statistiques préliminaires, et autres documents du GNB.

Les données **« confidentielles »** sont celles qui doivent être protégées en vertu de la législation, des lois ou des règlements. Cette catégorie s'applique aux fonds de renseignements qui pourraient causer un grave préjudice à une personne, à une organisation ou à un gouvernement s'ils étaient compromis.

Mentionnons **par exemple** les renseignements personnels sur la santé, les évaluations personnelles et les enquêtes, les examens provinciaux de 12^{e} année, les secrets industriels, les dossiers financiers, le secret professionnel des avocats et l'information de nature commerciale confidentielle provenant d'un tiers. Les secrets administratifs ou les conseils au ministre pourraient également s'insérer dans cette catégorie.

Les données **« hautement confidentielles »** sont les renseignements qui, s'ils étaient communiqués à l'extérieur du GNB, pourraient porter gravement atteinte à l'organisation, même jusqu'au point de défaillance. De tels fonds de renseignements pourraient, s'ils étaient compromis, causer un préjudice extrêmement grave à une personne, à une organisation ou à un gouvernement. La consultation des renseignements « hautement confidentiels » pourrait nécessiter une cote de sécurité.

Mentionnons par **exemple** les vulnérabilités des infrastructures essentielles, les casiers judiciaires, les documents relatifs aux informateurs de police et les renseignements « Protégé C » liés à des enquêtes criminelles. La consultation de ces renseignements pourrait nécessiter une cote de fiabilité ou de sécurité.

Tableau de classification des niveaux de cybersécurité

Classification du GNB	Commentaires	Norme fédérale canadienne
Information publique	Accessible sur les sites Web du GNB/données ouvertes	Information non classifiée
Information interne	Information liée aux activités du GNB, mais non publique	Protégé A
Information confidentielle (législation, lois ou règlements)	Renseignements personnels sur la santé, renseignements sur la santé mentale, conseils au ministre, secrets administratifs	Protégé B
Information hautement confidentielle (pourrait nécessiter une cote de sécurité)	Vulnérabilité des infrastructures essentielles, casiers judiciaires, protection des témoins	Protégé C

6 DIRECTIVES CONNEXES

BCI TI 9.01 – Propriété des données
BCI TI 9.02 – Classification des données
BCI TI 9.06 – Cryptage des données