

1 DIRECTIVE

- 1.01 Les organisations du GNB prendront les mesures qui conviennent pour faire en sorte que l'accès physique aux systèmes informatiques ou à l'infrastructure de TI soit accordé seulement aux personnes qui en ont besoin dans l'exercice de leurs fonctions.

2 OBJET

- 2.01 La présente directive a pour objet de faire en sorte que :
- il existe une protection contre les dommages physiques accidentels causés par des employés inexpérimentés ou contre les dommages intentionnels causés dans le but d'endommager l'installation;
 - tous les employés soient au courant des dangers et prennent des mesures positives pour mettre en application les restrictions d'accès sans s'exposer à un risque d'être la cible d'intrus;
 - les contrôles de l'accès physique soient à jour pour ce qui est des responsabilités du personnel et de la sensibilité des données protégées.

3 PORTÉE

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

4 RESPONSABILITÉ

- 4.01 Le **gestionnaire du site** est responsable de réviser, d'approuver et de tenir à jour les niveaux d'autorisation qui conviennent pour tous les employés du GNB dans tous les emplacements comptant une installation de TI, que ce soit sur place ou ailleurs.
- 4.02 Tous les employés sont responsables de respecter les mesures de protection, d'encourager les autres à faire de même et de signaler ou d'aborder les cas de non-respect.

5 DÉFINITIONS

- 5.01 **Contrôle de l'accès** désigne la mise en œuvre et l'application de mesures de contrôle visant à régir l'accès des employés et autres personnes aux systèmes et biens de TI et aux emplacements où ces systèmes sont hébergés ou utilisés.
- 5.02 **Infonuagique** désigne le traitement et le stockage de données ou de programmes ou l'accès à ceux-ci sur Internet, plutôt que l'exécution de ces fonctions à l'aide de matériel informatique et de logiciels hébergés physiquement à l'emplacement de votre organisation.

5.03 **Talonnage** désigne une atteinte à la sécurité physique commise lorsqu'une personne entre dans un local protégé dont la porte est normalement verrouillée en suivant de près une personne autorisée à y pénétrer.

6 **DIRECTIVES CONNEXES**

BCI TI 1.04 — Planification de site

BCI TI 8.02 – Sécurité des systèmes

BCI TI 8.03 – Identification et mots de passe des utilisateurs