Directive sur la cybersécurité : TI 8.02	Publié : 04/2019
Chapitre : Sécurité physique et sécurité des systèmes	Dernière révision : 01/2022
Objet : **SÉCURITÉ DES SYSTÈMES**	

1 DIRECTIVE

1.01 Pour les serveurs et les systèmes informatiques hôtes, les **Opérations de la TI** contrôleront et régiront ce qui suit :

- Contrôles de l'identification et de l'authentification des utilisateurs
- Accès et connexion des utilisateurs
- Autorisation d'exécution des applications par les utilisateurs

1.02 Seul le **Soutien de la TI** peut installer ou mettre à jour les logiciels d'exploitation, les logiciels d'application ou le matériel informatique, quels qu'ils soient.

1.03 Pour les systèmes informatiques reliés à un réseau :

- le **Soutien de la TI** doit approuver tout le matériel informatique ainsi que les logiciels d'exploitation et d'application qui seront installés ou mis à niveau;
- des contrôles de l'identification et de l'authentification des utilisateurs doivent être mis en place sur les ordinateurs personnels, et les utilisateurs « invités » ne doivent pas être autorisés.

1.04 Pour une installation de TI dont les activités exigent des échéanciers de production critiques (p. ex. société de services, production externalisée), le **Soutien de la TI** doit contrôler toutes les installations et mises à niveau de matériel informatique et de logiciels sur les systèmes personnels.

2 OBJET

La présente directive a pour objet de faire en sorte que :

- tous les utilisateurs qui ont recours à un système informatique en réseau ou relié à un serveur ou à un système hôte de l'organisation puissent être identifiés et soient autorisés à travailler sur ces systèmes;
- seuls des logiciels d'application et d'exploitation autorisés, soumis à des contrôles de sécurité et entièrement autorisés sont installés sur les systèmes de TI de l'organisation.

3 PORTÉE

3.01 La présente directive s'applique à tous les employés et tiers fournisseurs qui détiennent des responsabilités liées aux **Opérations de la TI** et au **Soutien de la TI**.

4 RESPONSABILITÉ

4.01 Les gestionnaires sont responsables d'informer les **Opérations de la TI** du statut de leurs employés et des responsabilités des employés qui nécessitent des autorisations précises.

4.02 Les **Opérations de la TI** sont responsables de contrôler les identifiants et les niveaux d'autorisation associés à chaque utilisateur.

4.03 Le **Soutien de la TI** est responsable de ce qui suit :

a) Planifier, mettre à l'essai et examiner l'ensemble du matériel informatique du système et des logiciels d'exploitation et d'application standard pour ce qui est des contrôles de sécurité et de l'exposition.

b) Veiller à ce que tous les logiciels d'exploitation et d'application installés sur les systèmes personnels et en réseau soient autorisés et sous licence.

4.04 Le **Soutien de la TI** est responsable de planifier, de mettre à l'essai et d'examiner tous les logiciels d'application personnalisés et les extensions pour ce qui est des contrôles de sécurité et de l'exposition du système.

5 DÉFINITIONS

5.01 **Autorisation d'administrateur** désigne une autorisation particulière à exécuter des tâches qui sont habituellement réservées aux personnes qui sont autorisées à modifier les logiciels d'exploitation et les options de l'environnement.

5.02 **Utilisateur invité** désigne une identification d'utilisateur qui permet à tout individu d'utiliser un système informatique sans avoir à s'identifier. Les utilisateurs invités sont généralement autorisés à effectuer des activités de base très limitées sur un ordinateur personnel ne disposant pas d'accès au réseau ni au système hôte.

6 DIRECTIVES CONNEXES

BCI TI 3.01 — Applications standards

BCI TI 3.03 — Logiciel non standard

BCI TI 9.03 – Contrôles de l'accès aux données

BCI TI 13.01 – Accès aux systèmes et utilisation acceptable des systèmes