Directive du Bureau du Chef de l'Information: TI 4.02	Publié: 02/2020
Chapitre: Gestion des systèmes	Dernière révision: 01/2022
Objet: **Gestion des utilisateurs en fonction de leur rôle**	

1 DIRECTIVE

1.01 En ce qui a trait au contrôle de l'accès au système,

a) tous les utilisateurs de TI se verront attribuer un ensemble normalisé de privilèges d'accès au système d'après un modèle défini par l'organisation de prestation de services de TI;

b) le gestionnaire de l'utilisateur doit demander les privilèges supplémentaires dont a besoin un utilisateur et la demande doit être approuvée par le responsable opérationnel.

1.02 En ce qui a trait au contrôle des applications et des données,

a) les processus de TI entraînant des paiements ou le transfert de biens doivent viser deux utilisateurs ou plus pour que le processus soit lancé et pour la validation ou l'approbation du processus avant sa réalisation;

b) le responsable d'une application ou de données doit approuver l'accès à l'application ou aux données nécessitant des autorisations particulières.

2 OBJET

2.01 La présente directive vise la mise en place de mesures de contrôle supplémentaires, plus précisément

- pour détecter les erreurs au moyen de processus en plusieurs étapes, pour limiter les possibilités de fraude ou de vol de la part d'employés et pour accroître la probabilité de détection lors des tentatives de fraude ou d'appropriation illicite de biens;
- pour protéger les ordinateurs et les réseaux de l'organisation contre une exposition accidentelle à des menaces extérieures.

3 PORTÉE

3.01 La présente directive s'applique à

a) tous les concepteurs d'applications et de processus;

b) tous les gestionnaires attribuant des responsabilités liées aux processus;

c) tous les opérateurs de systèmes jouissant de privilèges allant au-delà de ceux d'un utilisateur restreint.

4 RESPONSABILITÉ

4.01 L'organisation de prestation de services de TI assume, conjointement avec le responsable opérationnel, la responsabilité d'évaluer les demandes de privilèges additionnels à ceux du modèle de base défini de la part des utilisateurs.

4.02 L'organisation de prestation de services de TI et le responsable opérationnel ont la responsabilité

a) d'inclure plusieurs utilisateurs durant l'exécution de tout processus entraînant le transfert de fonds ou de biens;

b) de veiller à ce que les demandes ne nécessitent pas l'attribution de privilèges spéciaux pour être actives durant l'exécution des tâches, à moins que la tâche à exécuter ne nécessite de tels privilèges.

4.03 Chaque gestionnaire de service a la responsabilité de veiller à ce

a) qu'aucun employé du service ne jouisse de tous les privilèges requis pour l'exécution intégrale d'un processus contrôlé;

b) que les employés changeant de responsabilités au sein du service ou mutés hors du service soient démunis de tous les privilèges spéciaux leur ayant été accordés.

4.04 Tous les utilisateurs ayant besoin de privilèges supplémentaires pour l'exécution de tâches particulières ont la responsabilité de veiller à ce que ces privilèges soient actifs seulement durant l'exécution des tâches en question.

5 DÉFINITIONS

5.01 La **« séparation des tâches »** est un principe de sécurité qui assure l'organisation qu'une personne donnée ne peut commettre une infraction à la sécurité par elle-même.

5.02 Le principe du **« privilège minimal »** est un principe de sécurité qui assure l'organisation qu'un utilisateur ne jouit que des privilèges requis pour la tâche à exécuter sans plus.

6 DIRECTIVES CONNEXES

BCI TI 8.02 – Sécurité des systèmes

BCI TI 8.03 – Identification et mots de passe des utilisateurs

BCI TI 8.04 – Confidentialité et protection des renseignements personnels

BCI TI 9.03 – Mesures de contrôle de l'accès aux données

BCI TI 9.04 – Mesures de contrôle de la sécurité des applications

BCI TI 13.01 – Accès au système et utilisation acceptable du système

BCI TI 13.09 – Accès à distance – utilisateurs