Directive du Bureau du Chef de l'Information: TI 5.01	Publié: 02/2020
Chapitre: Gestion des données	Dernière révision: 02/2024
Objet: **Intégrité et validation du traitement des données**	

1 DIRECTIVE

1.01 Des mesures de contrôle doivent être en place pour tous les processus qui aboutissent à la création, à la manipulation, à la transmission ou au stockage de données afin de protéger l'intégrité des données contre une modification, une perte ou des dommages accidentels, intentionnels ou malveillants.

1.02 Des mesures de contrôle doivent être également en place pour détecter toute perte d'intégrité des données au moment où elle se produit afin de pouvoir intervenir rapidement pour récupérer ces données.

2 OBJET

2.01 La présente directive a pour objet de s'assurer que des mesures de contrôle sont en vigueur pour protéger les données contre des menaces possibles pour leur intégrité et pour détecter rapidement les atteintes à celle-ci. Chaque fois que des données sont créées, stockées, traitées ou transmises, elles doivent demeurer complètes et correctes du début à la fin de leur cycle de traitement.

3 PORTÉE

3.01 La présente directive s'applique à tous les employés qui participent à la manipulation, à la transmission, au traitement et au stockage des données.

4 RESPONSABILITÉ

4.01 Tous les employés sont responsables du maintien de l'intégrité des données pendant leur préparation, traitement, transmission et stockage. Quand ils préparent les spécifications pour ces processus, les employés sont responsables de déterminer les mesures de protection à intégrer dans les processus.

5 DÉFINITIONS

5.01 L'**intégrité des données** désigne la validité des données. Les données sont valides si elles sont exactes, à jour et complètes. Les données peuvent ne pas être valides pour les raisons suivantes :

- des erreurs de saisie;
- des erreurs de transmission survenues lors de leur envoi à un autre ordinateur ou à un serveur de fichiers au sein du même réseau;
- des défaillances du matériel informatique (p. ex. supports de données endommagés, écrasements de tête, pannes d'électricité ou pannes de système qui endommagent les données);
- des bogues logiciels des applications;
- des catastrophes environnementales (p. ex. incendie, dégâts des eaux, surtensions);
- une modification intentionnelle à des fins de gain personnel ou dans une

intention malveillante.

6 DIRECTIVES CONNEXES

BCI TI 5.03 – Gestion des services de tiers fournisseurs
BCI TI 8.01 – Sécurité physique et sécurité de l'infrastructure
BCI TI 8.02 – Sécurité des systèmes
BCI TI 9.04 – Contrôles de sécurité des applications