

<p>Directive du Bureau du Chef de l'Information : TI 13.02</p> <p>Chapitre : Responsabilités des utilisateurs</p> <p>Objet : Accès aux données et protection des données</p>	<p>Publié : 04/2019</p> <p>Dernière révision : 01/2022</p>
---	--

1 DIRECTIVE

1.01 Les utilisateurs peuvent accéder aux données auxquelles ils sont autorisés, à l'aide d'applications, de programmes, d'interfaces et de procédures autorisés par le GNB.

2 OBJET

2.01 La présente directive a pour objet de réduire au minimum les risques de corruption ou de perte de données causés par la création, la consultation, la mise à jour ou le traitement inappropriés de ces données.

3 PORTÉE

3.01 La présente directive s'applique à tous les utilisateurs autorisés à accéder aux systèmes informatiques du GNB et aux données du GNB.

4 RESPONSABILITÉ

4.01 Tous les utilisateurs doivent restreindre leur accès aux données à l'aide d'applications, de programmes, d'interfaces et de procédures autorisés par le GNB.

4.02 Le soutien technique de la TI doit :

- a) Consigner les applications, les programmes et les interfaces appropriés pour accéder aux données et fournir des procédures consignées visant la classification, la gestion et le stockage appropriés des données.
- b) Fournir un mécanisme de contrôle actif de la mise à jour des données ou des contrôles procéduraux des données partagées ou des documents pouvant être mis à jour par un seul utilisateur à la fois puis retournés à l'emplacement partagé après la mise à jour.

4.03 Les administrateurs de systèmes de TI sont chargés de gérer l'accès autorisé des utilisateurs aux données en fonction de la classification des données et de l'approbation du propriétaire des données. (Voir aussi la **DCS TI 9.03 – Contrôles de l'accès aux données.**)

5 DÉFINITIONS

5.01 Le terme « **extraction** » désigne une demande d'un utilisateur à un mécanisme de contrôle des données afin d'empêcher que des données soient modifiées par un autre utilisateur. Si la demande d'extraction est acceptée, l'utilisateur peut mettre à jour les données en place ou les copier, modifier la

copie et remplacer l'original par la copie mise à jour. Un contrôle rigoureux des données peut empêcher que des données soient modifiées par quiconque jusqu'à ce qu'elles soient extraites, et alors l'utilisateur qui les a extraites est le seul à pouvoir les modifier. Un contrôle procédural des données peut permettre à un utilisateur de déterminer les données qui sont actuellement extraites pour la mise à jour, mais il appartient aux autres utilisateurs de vérifier l'état actuel des données et d'éviter de mettre à jour des données qui sont considérées comme extraites.

- 5.02 « **Enregistrement** » désigne une demande de l'utilisateur qui a réalisé une extraction réussie du mécanisme de contrôle des données afin de supprimer les restrictions imposées par l'extraction. La demande d'enregistrement est faite par l'utilisateur en contrôle après avoir effectué les mises à jour nécessaires et remplacé les données.

6 DIRECTIVES CONNEXES

BCI TI 5.02 – Sauvegarde et stockage

BCI TI 9.01 – Propriété des données

BCI TI 9.02 – Classification des données

BCI TI 9.03 – Contrôles de l'accès des données

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

BCI TI 13.03 – Mots de passe

BCI TI 14.01 – AVEC : Dispositifs et systèmes d'exploitation acceptables

BCI TI 14.02 – AVEC : Accès aux systèmes et utilisation acceptable des systèmes