Directive du Bureau du Chef de l'Information : TI 14.11	Publié : 04/2020
Chapitre : Gestion des appareils mobiles	Dernière révision : 01/2024
Objet : Sécuriser les appareils mobiles en déplacement	

1 DIRECTIVE

1.01 Les employés de toutes les parties du gouvernement qui voyagent à l'extérieur du milieu du travail sont responsables de la protection des appareils technologiques et de l'information du GNB qui leur ont été attribués.

Les appareils mobiles sont notamment :

- les ordinateurs portables;
- les tablettes et les ordinateurs blocs-notes;
- les cellulaires, les assistants numériques personnels et les appareils BlackBerry;
- les clés USB et les disques durs externes.

2 OBJET

2.01 La présente directive a pour objet de garantir que l'information du gouvernement demeure protégée pendant que les employés voyagent à l'extérieur du milieu de travail.

3 PORTÉE

3.01 Le présent énoncé de directive et procédure s'applique à toutes les personnes qui accèdent aux ressources et à l'information du GNB avec des appareils mobiles du GNB pendant un voyage autorisé à l'extérieur de la province.

4 RESPONSABILITÉ

4.01 Les employés du GNB (ou leurs gestionnaires) devraient aviser l'AMSI (agent ministériel de la sécurité de l'information) et l'organisation de prestation de services de TI (OPST) de tout projet de voyage à l'extérieur de la province : un préavis d'au moins trois (3) semaines est recommandé avant le départ pour des destinations à risque élevé (voir : Conseils aux voyageurs et avertissements - Voyage.gc.ca pour les destinations à risque élevé). Le OPST partagera et cette information avec l'AMSI concerné et avec d'autres personnes, selon les besoins, pour s'assurer qu'ils seront disponibles pour soutenir les voyageurs.

4.02 Les responsabilités ci-dessous incombent à l'employé du GNB (voyageur).

Avant le voyage

a) Passer en revue les avertissements pertinents pour les voyageurs, contenus dans les Conseils aux voyageurs et avertissements du gouvernement du Canada (voyage.gc.ca);
b) Prendre connaissance de la documentation fournie par son AMSI;
c) Prendre les précautions appropriées contre les risques potentiels;
d) Limiter les données stockées sur les appareils au strict nécessaire.

Pendant le voyage

a) Éviter d'utiliser les appareils peu fiables (comme l'équipement d'un hôte étranger ou les bornes);

b) Ne pas se connecter à des réseaux peu fiables (cafés, WIFI d'hôtel, etc.) :

- pour se connecter de manière sécurisée à l'information et aux ressources du GNB en utilisant un réseau peu fiable, utiliser un emplacement privé et un canal de communication sécurisé (comme un RPV),

c) signaler tous les problèmes ou toutes les difficultés au OPST dès qu'ils se produisent.

Après le voyage

a) Remettre les appareils au OPST aux fins d'analyse criminalistique, s'il y a lieu;

b) remplir le questionnaire de retour de voyage ou participer à une séance de bilan du voyage.

4.03 Les responsabilités ci-dessous incombent au OPST (p. ex. SNB).

Avant le voyage

a) Évaluer le niveau de cybersécurité nécessaire pour la région de destination à l'époque du voyage;

b) Configurer adéquatement les appareils mobiles avant le départ (cela peut comprendre l'attribution d'appareils de remplacement temporaires, à la configuration sur mesure, à utiliser pendant le voyage. Au besoin, le OPST peut également créer des comptes d'utilisateur temporaires et d'autres justificatifs d'identité);

c) Assurer le chiffrement de toutes les données stockées sur les appareils emportés en voyage, sous réserve des lois régissant les données éventuellement en vigueur à la destination.

Pendant le voyage

a) Assurer le soutien technique en cas de difficultés ou de problèmes de TI signalés par les voyageurs;

b) Comme il convient pour les destinations à risque élevé, surveiller le réseau, les fichiers et l'activité des appareils liée à des appareils connectés à distance;

c) Effacer à distance toutes les données sur les appareils mobiles du GNB dont la perte est signalée par un employé.

Après le voyage

a) Effectuer l'analyse criminalistique des appareils fournis par le GNB, s'il y a lieu;

b) Recueillir les questionnaires de retour de voyage et/ou animer une séance de bilan.

4.04 Appareils mobiles gérés par le GNB

- Tous les appareils gérés par le GNB qui contiennent des renseignements personnels sont toujours soumis aux exigences du GNB en matière de soutien.
- Tous les appareils gérés par le GNB sont soumis à leur récupération sans préavis par le OPST.
- Toutes les données personnelles figurant sur les appareils gérés par le GNB peuvent être soumises à un examen technique ou effacées pour raisons de sécurité.
- L'utilisation d'appareils autres que ceux du GNB pour accéder à des renseignements du GNB pendant les voyages au moyen d'Exchange, par exemple, n'est pas acceptable.

4.05 Personnes-ressources

Pour les questions de soutien en TI, communiquez avec le OPST.

Pour les questions sur la sécurité personnelle ou les obligations légales, communiquez avec le ministère de la Sécurité publique, Bureau du conseiller provincial en matière de sécurité.

Pour les conseils et le soutien d'ordre général, communiquez avec votre AMSI. Si votre AMSI n'est pas disponible ou si vous ne le connaissez pas, communiquez avec Finances et Conseil du Trésor, Bureau du chef de la sécurité de l'information.

5 DÉFINITIONS

- **AMSI –** agent ministériel de la sécurité de l'information
- **Chiffrement –** le chiffrement est le processus qui consiste à coder un message ou de l'information de façon à ne permettre leur accès qu'aux parties autorisées et à en interdire l'accès à celles qui ne le sont pas.
- **Informatique légale –** domaine de la criminalistique numérique relatif aux preuves trouvées dans les ordinateurs et les supports de stockage numériques.
- **Fournisseur de services de technologie de l'information** (OPST) **–** organisation qui offre des services visant à accéder au réseau du GNB, à l'utiliser ou à y participer.
- **Effacement sécurisé –** effacement en toute sécurité des données sur un ordinateur ou un appareil numérique.
- **Réseau privé virtuel** (VPN) **–** réseau qui étend un réseau privé dans un réseau public et qui permet aux utilisateurs d'envoyer et de recevoir des données dans des réseaux partagés ou publics comme si leurs

appareils informatiques étaient directement connectés au réseau privé.

6 DIRECTIVES CONNEXES