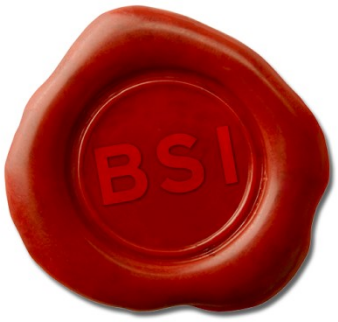
Guide

Déplacement sécuritaire avec équipement informatique



Bureau de sécurité de l'information
2018-07-23

UNIVERSITÉ LAVAL
Bureau de sécurité de l'information

Dans une perspective de développement durable et de réduction de notre empreinte écologique, le Bureau de sécurité de l'information (BSI) vous incite fortement à ne pas imprimer le présent document et à consulter la version électronique.

Guide - Déplacement sécuritaire avec équipement informatique – Juillet 2018

Table des matières

Introduction

Ce guide vise à vous sensibiliser sur les moyens sécuritaires à utiliser pour assurer la sécurité de vos équipements informatiques lors de vos déplacements dans la province, au Canada ou à l'international dans le cadre de vos activités en lien avec l'Université Laval.

Nous vous invitons à en prendre connaissance tant pour les recommandations avant le départ qu'à votre retour.

Le répondant de la sécurité de l'information (RS) de votre unité peut vous assister dans cette démarche.

Avant de partir

1. **Renseignez-vous sur les lois régissant la propriété intellectuelle, les données numériques et les données cryptées dans les pays que vous visitez**
    - Se familiariser avec la législation locale, ainsi qu'avec la réglementation pour l'entrée sur le territoire et la sortie;
    - La loi peut viser non seulement les données, mais aussi les logiciels, les applications et le matériel informatique et le support de stockage.

2. **Emportez seulement les informations nécessaires pour votre voyage**
    - Pour limiter les conséquences d'une perte ou d'un vol d'information sensible, n'emportez que les informations essentielles au voyage.

3. **Utilisez de préférence du matériel dédié aux missions**
    - Certaines unités mettent à la disposition de leurs employés des équipements réservés exclusivement au voyage. Il faut que vous vérifiiez auprès de l'assistance technique de votre unité si vous pouvez vous procurer ce matériel pour votre voyage;
    - Ces appareils (ordinateurs, téléphones intelligents, tablettes, supports amovibles, etc.) ne doivent pas contenir d'autres informations que celles dont vous avez besoin durant votre voyage;
    - Il est recommandé que le matériel dédié dispose d'une configuration minimale et qu'il ne contienne que les données et les logiciels requis pour le voyage.

4. **Faites la mise à jour de tout logiciel de vos équipements**
    - Assurez-vous d'avoir mis à jour tout logiciel antivirus avant votre départ;
    - Assurez-vous d'avoir installé les correctifs les plus récents du système d'exploitation et des applications. En cas d'utilisation d'un ordinateur portatif ou d'une tablette d'entreprise, consultez le service informatique de votre unité afin de vous assurer que ces mises à jour sont appliquées;
    - Assurez-vous que tout le matériel et tous les logiciels nécessaires sont installés pour éviter d'avoir à les acheter ou à les télécharger au cours du déplacement.

5. **Sauvegardez les données que vous planifiez emporter durant votre voyage**
    - En sauvegardant ces données dans un lieu sûr, il vous sera ainsi possible de récupérer vos informations à votre retour en cas de perte, de vol ou de saisie de vos équipements.

6. **Évitez de voyager avec des données sensibles**
    - Il est préférable d'accéder aux données sensibles durant votre voyage en utilisant l'accès à distance au réseau de l'Université avec une liaison sécurisée (VPN);
    - Les agents des services frontaliers sont légalement autorisés à faire des fouilles et des saisies à l'égard de toute personne qui entre dans leur pays ou qui en sort.

7. **Chiffrez, si c'est possible, les données stockées sur vos appareils**

Important

Certaines législations locales interdisent l'utilisation de logiciels de chiffrement ou même l'entrée d'un appareil contenant des données chiffrées sur leur territoire. Vérifiez cette information avant votre déplacement.

8. **Utilisez un filtre de protection-écran pour votre ordinateur**

- Cela vous permettra de travailler sur votre ordinateur, durant vos trajets, en toute discrétion.

9. **Marquez vos appareils d'un signe distinctif**

- Cela vous permet de surveiller votre matériel et de vous assurer qu'il n'y a pas eu d'échange, notamment pendant le transport;
- vous devrez également apprendre à détecter les manipulations. Il arrive souvent que les voleurs échangent simplement un équipement contre un autre similaire, de telle sorte que le vol ne paraisse pas immédiatement;
- Il est conseillé d'ajouter un signe distinctif sur tous les équipements ainsi que sur leurs housses. De cette manière, un vol sera immédiatement constaté.

10. **Activez la fonctionnalité de géolocalisation et installez un logiciel antivol si c'est possible**

- Certains équipements disposent d'options de localisation automatique et de logiciels antivol. Il est fortement recommandé de se familiariser avec ces options et d'envisager la possibilité de les activer.

Durant votre déplacement

1. **Protégez vos appareils, supports et fichiers**
    - Gardez vos appareils électroniques dans votre bagage de cabine afin d'éviter de les perdre ou de les endommager durant votre voyage;
    - Ne perdez jamais de vue vos appareils et ne les laissez jamais dans un bureau ou dans la chambre d'hôtel (même dans un coffre).
2. **Protégez l'accès au contenu de vos appareils par des mots de passe complexes et difficiles à deviner**
    - Configurer un mot de passe pour pouvoir accéder au contenu de vos appareils. Ce mot de passe doit être constitué d'au moins huit (8) caractères et contenir des caractères d'au moins deux (2) des catégories suivantes :
        - Lettres majuscules et minuscules: A, B, C, … Z, a, b, c, … z
        - Chiffres : 0, 1, 2, … 9
        - Caractères spéciaux : $%/?&*()
        - Il ne doit pas contenir d'espace blanc.
3. **Ne vous séparez pas de vos équipements**
    - Si vous devez vous séparer de votre téléphone intelligent ou de votre tablette, conservez avec vous la carte SIM.
4. **Pensez à effacer l'historique de vos appels et de vos navigations**
    - Outre l'historique, il faut effacer les données laissées en mémoire cache, fichiers de témoins (cookies), mots de passe d'accès aux sites Web et fichiers temporaires.
5. **Détruisez les informations non nécessaires de manière sécuritaire**
    - Si vous n'avez plus besoin de certaines informations sensibles pour le restant de la période de voyage, veuillez les détruire de manière sécuritaire. Ainsi, ils ne pourront pas être récupérées par autrui en cas de vol ou de perte.
    - **En cas d'inspection ou de saisie par les autorités, informez dès que possible le répondant en sécurité de l'information (RS) de votre unité**
    - Fournissez les mots de passe et clés de chiffrement si vous y êtes contraint par les autorités locales puis alertez votre Responsable de sécurité (RS).
6. **N'utilisez pas les équipements qui vous sont offerts (clés USB)**
    - Les clés USB peuvent contenir des logiciels malveillants et ils présentent un moyen d'infection largement utilisé par des personnes ou des organismes malveillants.

7. **Ne connectez pas vos équipements à des postes ou des périphériques informatiques qui ne sont pas de confiance**
    - Tout équipement qui se branche sur un port USB peut être un dispositif de stockage et risque de cacher un maliciel (lecteurs MP3, téléphones intelligents, lecteurs de disques durs externes, etc.);
    - Méfiez-vous des échanges de documents (exemple : par clé USB lors de présentations ou lors de colloques). Emportez une clé destinée à ces échanges et jetez-la après usage.

8. Évitez d'utiliser une connexion Internet sans fil publique

- Éviter d'utiliser une connexion Internet sans fil publique et de transmettre des informations sensibles qui peuvent être facilement interceptées par ces connexions;
- Lorsqu'il vous est possible, utilisez une connexion câblée plutôt qu'un réseau sans fil public. La connexion câblée est habituellement plus sécuritaire qu'un réseau sans fil gratuit.

9. Désactivez la fonction Bluetooth

- Désactivez la fonction Bluetooth de votre appareil lorsque vous ne l'utilisez pas. Certains appareils permettent la connexion automatique avec d'autres appareils Bluetooth et ainsi établir une connexion non autorisée à votre insu.

10. Ne rechargez pas vos équipements sur les bornes électriques libre-service

- Évitez de connecter votre téléphone à un ordinateur ou à un appareil qui ne vous appartient pas, comme les ports d'alimentation dans les hôtels;
- Certaines de ces bornes peuvent avoir été conçues pour copier les documents à votre insu;
- Pour recharger votre téléphone intelligent ou tablette, utilisez votre ordinateur personnel ou un port d'alimentation directement branché au mur.

Que faire en cas de vol

En cas de perte ou de vol d'un équipement ou d'information :

- Rédigez immédiatement une liste de ce qui vous a été volé;
- Demandez conseil à l'ambassade du Canada ou au service consulaire du Canada avant toute démarche auprès des autorités locales;
- Portez ensuite plainte auprès des autorités de la police locale;
- Informez le répondant en sécurité de l'information (RS) de votre unité de tout équipement informatique ou de données sensibles ayant été volés (ordinateur, tablette, téléphone intelligent, clé USB, disque dur externe, CD/DVD).

Avant votre retour

1. Transférez vos données

- Transférez les données contenues dans vos équipements informatiques que vous aviez en voyage sur le réseau de votre organisation à l'aide d'une connexion sécurisée.

2. Effacez l'historique de vos appels et de vos navigations

- Effacez l'historique de vos appels et de vos navigations sur l'ensemble de vos appareils intelligents (tablette, téléphone) ainsi que sur votre ordinateur.

Après votre retour

1. **Changez tous les mots de passe**
   - Changez tous les mots de passe que vous avez utilisés pendant votre voyage, car ils peuvent avoir été interceptés à votre insu;
   - Réinitialisez tous les identifiants des comptes d'accès locaux et à distance de vos appareils, ainsi que tous vos comptes, y compris les comptes personnels (même si vous ne les avez pas utilisés durant votre déplacement), qui ont des noms d'utilisateur et mot de passe semblables.

2. **Effectuez un inventaire de vos données et équipements**
   - Vérifiez la présence de tous les équipements et les données que vous avez apportés avec vous pendant votre voyage.

3. **Signalez tout élément SDI notable**
   - Rapportez à votre gestionnaire responsable de la sécurité de l'information (GRS) tout élément notable, concernant la sécurité de l'information qui s'est déroulé pendant le voyage.

4. **Effacez complètement votre équipement de déplacement**
   - procédez à l'effacement sécuritaire de tout équipement qui vous a été prêté pour votre usage durant le déplacement.

5. **Analysez ou faites analyser vos équipements**
   - Ne connectez pas les appareils au réseau de l'Université avant d'avoir fait ou fait faire les vérifications nécessaires quant à l'existence d'éventuels maliciels dans vos équipements électroniques (ordinateur, tablette, téléphone intelligent, clé USB, disque dur externe, CD/DVD).

Bureau de sécurité de l'information
Pavillon Agathe-Lacerte
1100, avenue de la Médecine
Bureau 1040
Université Laval
Québec (Québec) G1V 0A9
Tél. : 418 656-2131
Téléc. : 418 656-2737
C. élec. : info@bsi.ulaval.ca