[redacted]

De: [redacted]
Envoyé: 2 septembre 2021 10:13
À: [redacted]
Objet: TR: Avis informatique - COVID-19, Mesures de sécurité relatives au télétravail

Importance: Haute

De : AVIS INFORMATIQUE
Envoyé : 18 mars 2020 11:22
Objet : Avis informatique - COVID-19, Mesures de sécurité relatives au télétravail
Importance : Haute

AVIS
INFORMATIQUE

Mesures de sécurité et de confidentialité dans le cadre du télétravail

Les ordinateurs portables renferment souvent de l'information personnelle, confidentielle ou stratégique. Le télétravailleur demeure assujetti aux règles en vigueur et doit, notamment, respecter la politique et le cadre de gestion ministériel de la sécurité de l'information ainsi que les autres lois afférentes.

Même si les employés peuvent devoir travailler à leur domicile ou ailleurs, avec des documents sensibles, sous format papier ou support informatique; ils doivent le faire dans un souci de préserver la confidentialité de l'information.

Dans le cas où le personnel doit travailler à domicile avec des documents papier ayant un contenu stratégique et confidentiel pour l'organisation, ceux-ci devraient être conservés dans des endroits jugés sécuritaires par l'employé lorsqu'ils ne sont pas utilisés.

Les documents de nature stratégique ou confidentielle ne doivent pas être stockés sur les ordinateurs personnels. Le ministère offre des solutions de télétravail par VPN, qui assurent une sécurité des informations pour les cas jugés incontournables.

Si, dans l'exercice de vos fonctions, vous avez à faire du télétravail ou à voyager avec des portables appartenant au ministère, vous devenez responsable de ses équipements mobiles. On s'attend à ce que le même niveau de protection soit appliqué, comme si l'équipement mobile se trouvait dans les édifices du ministère, conformément à la Politique ministérielle de sécurité de l'information. Le ministère a le devoir de protéger

toute information dont il est responsable, peu importe l'endroit où elle se trouve et la forme qu'elle revêt, et ce, tout au long de son cycle de vie.

Il faut donc garder à l'esprit que tout portable ayant accès au réseau du ministère peut devenir un élément de risque potentiellement exploitable. Lorsque vous êtes dans un cadre de travail extérieur, vous pourriez être plus exposé à des personnes mal intentionnées et, par conséquent, plus susceptible d'être victime d'un incident de sécurité de l'information.

Des mesures spécifiques propres à chacune des directions générales ou des organismes peuvent aussi s'appliquer.

Bris ou perte d'un ordinateur portable

En cas de non-fonctionnement ou de bris d'un portable, l'utilisateur doit, sans délai, informer le technocentre du ministère.

Si un ordinateur portable se retrouve entre de mauvaises mains, cela peut engendrer de très graves conséquences. Voilà pourquoi toute perte doit être signalée dans les plus brefs délais à l'adresse courriel suivante : cogi@msp.gouv.qc.ca.

Conséquences

Il est à noter que le fait d'avoir accès aux ressources informationnelles ministérielles, par l'entremise d'ordinateurs portables, est un privilège et non un droit. Si un employé ne respecte pas la ligne de conduite décrite dans sa politique de sécurité de l'information, le ministère conserve la possibilité de révoquer ce privilège.

Tout utilisateur qui enfreint les dispositions de la Politique de sécurité de l'information s'expose à des mesures administratives ou disciplinaires en fonction de la gravité et des conséquences de son geste. Ces mesures peuvent inclure la révocation du privilège d'utilisation d'un appareil mobile, une suspension ou un congédiement, et ce, conformément aux dispositions des lois et règlements, des conventions collectives et des contrats de travail en vigueur.

Une brèche de sécurité peut être causée dans le réseau du ministère par un utilisateur bien intentionné, mais mal informé. Faites preuve de vigilance et appliquez les bonnes pratiques ci-dessous.

Bonnes pratiques

√ Utiliser les moyens de communication sécurisés offerts par le ministère (VPN) lorsqu'on ne travaille pas dans ses locaux.

√ Sauvegarder uniquement les données essentielles sur le portable.

√ Effacer de son portable toute information sensible lorsque cette dernière n'est plus requise.

Mauvaises pratiques

X Brancher un média portable (clé USB, CD-ROM, disque dur externe) de source inconnue sur son portable.

X Copier de l'information, même partielle, appartenant au ministère, sur de l'équipement qui n'appartient pas au ministère.

X Modifier la configuration des ordinateurs portables ou des logiciels installés et/ou désactiver les mesures de sécurité.

X Consulter des dossiers confidentiels dans un endroit public (cela facilite l'espionnage).

Documents de référence : Politique ministérielle de sécurité de l'information