JUILLET 2020

FEUILLE-INFO

SUR LA PROTECTION DE LA VIE PRIVÉE

Le télétravail pendant la pandémie de COVID-19

De nombreuses organisations du gouvernement et du secteur public ont dû fermer leurs bureaux précipitamment en raison de la crise de santé publique causée par la COVID 19. Sans avertissement, les employés se sont retrouvés à la maison, travaillant souvent dans des conditions improvisées. Une pareille situation peut présenter de nouveaux problèmes et risques sur le plan de la vie privée, de la sécurité et de l'accès à l'information.

Bien que la situation actuelle soit sans précédent et évolue rapidement, les lois ontariennes sur l'accès à l'information et la protection de la vie privée restent en vigueur. Votre organisation doit donc prendre des mesures rapides et efficaces pour réduire les risques associés à cette nouvelle réalité. La présente feuille-info décrit des pratiques exemplaires à suivre pour le télétravail afin de protéger la vie privée et d'assurer l'accès à l'information.

POLITIQUES DE TÉLÉTRAVAIL

Avec les membres de votre personnel responsables des services informatiques, de la sécurité, de la protection de la vie privée et de la gestion de l'information, examinez et mettez à jour vos politiques de télétravail afin de minimiser les risques pour l'accès à l'information, la vie privée et la sécurité, car la situation a évolué depuis la rédaction de ces politiques.

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Si vous n'avez pas adopté de telles politiques, vous devriez en rédiger en adaptant vos politiques actuelles sur la protection de la vie privée, la sécurité et l'accès aux données en fonction des conditions particulières de la situation actuelle, où presque tous les employés travaillent à la maison.

COMMUNICATION AVEC LE PERSONNEL

Rappelez ce qui suit à votre personnel :

- les exigences législatives et les politiques internes concernant l'accès à l'information, la protection de la vie privée, la sécurité et la gestion de l'information s'appliquent également au télétravail;
- il faut signaler immédiatement toute atteinte à la sécurité de l'information ou à la vie privée (c'est-à-dire les incidents où des renseignements personnels sont perdus ou volés, ou encore recueillis, utilisés ou divulgués sans autorisation).

Donnez à votre personnel :

- les coordonnées mises à jour de personnes pouvant leur fournir du soutien technique et administratif (par exemple, personnel responsable des services informatiques, de la sécurité, de la gestion des documents ainsi que de l'accès à l'information et de la protection de la vie privée);
- des conseils pratiques sur la façon de déceler les fraudes, l'hameçonnage et d'autres cyberattaques et de se prémunir contre eux (par exemple, en montrant au personnel comment déceler les signes révélateurs de courriels frauduleux et en lui rappelant de ne pas ouvrir les pièces jointes ni cliquer sur des hyperliens provenant d'expéditeurs inconnus).
    - Voir la feuille-info du CIPVP sur l'hameçonnage intitulée *Protect Against Phishing* (en anglais) pour les pratiques exemplaires à ce sujet : **https://www.ipc.on.ca/wp-content/uploads/2019/07/fs-tech-protect-against-phishing-e.pdf**

ACCÈS À DISTANCE AUX RÉSEAUX ET À L'INFORMATION

Si possible, permettez l'accès sécurisé à distance à vos réseaux, bases de données et comptes de courriel (par exemple, en obligeant le personnel à utiliser des contrôles d'accès efficaces comme l'authentification à facteurs multiples, ainsi qu'un réseau privé virtuel avec chiffrement de bout en bout).

Interdisez à votre personnel qui dispose de l'accès sécurisé à distance :

- d'utiliser un accès WiFi non sécurisé;
- de retirer du bureau des renseignements personnels (sur support électronique ou papier) sans autorisation.

Compte tenu des risques accrus associés au télétravail, vous devriez examiner les contrôles d'accès de votre organisation afin de vous assurer que les membres de votre personnel ont accès uniquement aux renseignements personnels dont ils ont besoin pour leurs fonctions.

MATÉRIEL ET LOGICIELS

Appareils fournis par l'organisation

Déterminez les technologies et les autres ressources (comme les ordinateurs et téléphones portables, les supports USB sécurisés, les imprimantes, les logiciels, etc.) dont les membres de votre personnel ont besoin à des fins de télétravail.

Votre organisation devrait idéalement leur fournir les logiciels et le matériel dont ils ont besoin pour travailler à la maison. Cela permet de réduire considérablement les risques pour la vie privée et la sécurité associés à l'utilisation d'appareils et de logiciels personnels, notamment de logiciels de sécurité qui ne répondent pas aux normes de l'industrie ou qui sont périmés et d'appareils partagés.

Les appareils que votre organisation met à la disposition des membres de son personnel devraient être dotés de logiciels de sécurité à jour ainsi que des applications et des autres ressources dont ils ont besoin pour remplir leurs fonctions tout en assurant la protection de la vie privée et de la sécurité.

Ces appareils et les logiciels doivent être configurés correctement, de préférence par votre personnel des services informatiques. Si l'utilisation de plateformes externes de communication et de services d'infonuagique est autorisée ou requise, assurez-vous que votre personnel sait comment les installer, les configurer et les utiliser en toute sécurité. Par exemple, pour les séances de vidéoconférence, il devrait y avoir des contrôles d'accès par mot de passe et des restrictions concernant le partage de pages-écrans et les enregistrements.

Le personnel ne devrait pas télécharger des logiciels ou applications ni les installer dans des appareils fournis par votre organisation sans autorisation. De nombreux logiciels et applications populaires présentent des vulnérabilités en matière de sécurité qui peuvent exposer votre organisation à des risques inutiles.

Appareils personnels

Si vous n'êtes pas en mesure de fournir du matériel et des ressources connexes à tous les membres de votre personnel, et si certains d'entre eux doivent se servir d'appareils personnels à des fins professionnelles, envisagez les mesures à prendre pour mieux protéger les renseignements qui seront consultés et utilisés au moyen de ces appareils et qui y seront sauvegardés. Par exemple, le logiciel de sécurité installé dans les ordinateurs domestiques pourrait être moins performant que celui que vous utilisez au bureau et nécessiter une mise à niveau.

Si les membres de votre personnel doivent utiliser leurs appareils personnels à des fins professionnelles :

- rappelez-leur de prendre des précautions appropriées pour protéger les renseignements personnels, notamment en installant les caractéristiques de sécurité nécessaires, en activant et en mettant à jour le logiciel antivirus et en sécurisant les connexions WiFi;
- si vous ne disposez pas d'outils d'accès sécurisé à distance, demandez-leur de séparer et de sécuriser tous les documents liés à leur travail dans les appareils partagés qu'ils utilisent à la maison (par exemple, en sauvegardant des fichiers protégés par mot de passe dans des appareils personnels à un emplacement différent des documents personnels, afin que les autres membres de leur famille ne puissent y accéder);
- dressez un plan de gestion de la destruction sécuritaire des documents professionnels une fois terminée la période de conservation pertinente.

COMMUNICATION PAR COURRIEL

Demandez aux membres de votre personnel d'utiliser uniquement les comptes de courriel de votre organisation dans toute la mesure du possible.

Rappelez-leur de protéger tous les documents contenant des renseignements personnels avant d'envoyer des courriels en prenant les mesures suivantes :

- sécuriser les renseignements personnels dans les appareils professionnels ou personnels (par exemple, en chiffrant ou en protégeant par mot de passe les pièces jointes et en communiquant les mots de passe séparément, par un moyen de communication ou dans un message différent);
- s'il est impossible de sécuriser les renseignements personnels, obtenir le consentement préalable du particulier concerné par ces renseignements avant de les transmettre;
- vérifier l'identité du destinataire et veiller à utiliser la bonne adresse de courriel (par exemple, en envoyant un courriel d'essai à l'avance pour confirmer qu'il parvient au bon destinataire);
- vérifier que le courriel contient uniquement des renseignements pertinents pour le destinataire en question.

ESPACES DE TRAVAIL À DOMICILE

Conseillez aux membres de votre personnel d'aménager un espace de travail privé à la maison ou à un emplacement convenu avec leur chef de service.

Exigez que toutes les mesures raisonnables soient prises afin que les autres occupants du domicile ou de l'autre lieu de travail convenu ne puissent pas lire le contenu affiché à l'écran ni entendre les conversations téléphoniques ou vidéo comportant des renseignements personnels ou d'autres renseignements délicats.

Rappelez à votre personnel :

- de sécuriser les appareils informatiques personnels et ceux fournis par votre organisation après usage ou avant de les laisser sans surveillance;
- de ne jamais laisser leurs appareils informatiques à la vue de tous ou non sécurisés hors de leur domicile;
- de ne pas travailler dans un endroit public où il y a un risque plus élevé d'écoute illicite ainsi que de vol et de perte de matériel;
- de protéger leurs appareils par mots de passe et chiffrement.

DOCUMENTS SUR PAPIER ET SUR D'AUTRES SUPPORTS

Rappelez aux membres de votre personnel de prendre des précautions appropriées pour protéger les documents sur papier et d'autres supports qui contiennent des renseignements personnels (par exemple, des photos, des enregistrements audio ou vidéo, des disques durs et des clés USB), notamment les suivantes :

- ne pas laisser de renseignements personnels non sécurisés ou sans surveillance lorsqu'ils s'absentent de leur espace de travail;
- sauvegarder de façon sécurisée tous les documents qui contiennent des renseignements personnels, sans égard à leur support;
- ne pas imprimer inutilement des documents contenant des renseignements personnels;
- ne pas jeter de documents sur papier qui contiennent des renseignements personnels (par exemple, à la poubelle ou au recyclage);
- conserver de façon sécurisée les renseignements personnels s'il est impossible de suivre à domicile les protocoles de destruction sécurisée, jusqu'à ce qu'il soit possible d'obtenir l'accès à des services de destruction sécurisée de documents.

Votre organisation devrait dresser un plan de destruction sécurisée de tout document contenant des renseignements personnels, sans égard au

support, une fois terminée la période de conservation établie. Aux termes de ce plan, les membres de votre personnel pourraient être autorisés à utiliser les installations de destruction de documents de votre bureau s'il est possible de le faire en toute sécurité.

DROITS RELATIFS À L'ACCÈS À L'INFORMATION

Votre organisation demeure tenue de permettre l'accès à l'information et de prendre des mesures raisonnables pour consigner et conserver les documents, même si votre personnel travaille à domicile.

Afin que votre organisation respecte ces obligations, vous devriez rappeler ce qui suit aux membres de votre personnel :

- tous les documents liés au travail demeurent assujettis aux lois sur l'accès à l'information, qu'ils se trouvent dans des appareils ou sur des supports fournis par l'organisation ou personnels;
- les activités professionnelles devraient être consignées; par exemple, des notes détaillées doivent être prises concernant toutes les décisions importantes, et tous les documents professionnels doivent être conservés;
- il est important d'observer de bonnes pratiques de gestion des documents, notamment en utilisant des conventions approuvées pour les noms de fichiers afin que les documents puissent être bien gérés et faciles à localiser;
- tous les documents professionnels doivent être numérisés et transférés dans des systèmes et registres professionnels dès que possible;
- une copie de sécurité des documents professionnels qui se trouvent dans un ordinateur ou des dispositifs de stockage personnels doit être effectuée.

STRATÉGIE À LONG TERME

Afin de continuer à répondre à ses besoins opérationnels tout en observant les lois sur l'accès à l'information et la protection de la vie privée, votre organisation devrait élaborer une stratégie de télétravail à long terme. Les politiques, les pratiques et la formation à distance devraient aborder des questions essentielles telles que les suivantes :

- l'utilisation d'appareils informatiques personnels;
- la marche à suivre pour récupérer les documents professionnels et les autres informations auprès des membres du personnel qui quittent l'organisation pendant la pandémie;
- le transfert et la conservation sécurisés de documents, y compris de renseignements personnels;

- l'élimination sécurisée des documents et appareils, y compris des appareils personnels, utilisés à des fins professionnels pendant la pandémie;
- le retour des documents et des appareils au bureau, et la mise à jour des dossiers et registres internes;
- la gestion des demandes d'accès à l'information, y compris l'exigence de mener des recherches raisonnables pour localiser les documents;
- la surveillance et l'évaluation de l'efficacité des mesures d'accès à l'information et de protection de la vie privée (et de sécurité) dans un contexte de télétravail, et l'amélioration continue de ces mesures en fonction de critères pratiques et d'expériences vécues.

RESSOURCES

Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario

La protection de la vie privée et les appareils mobiles, mai 2014, **https://www.ipc.on.ca/wp-content/uploads/2017/06/safeguarding-privacy-on-mobile-devices-f.pdf**

Messagerie instantanée et comptes de courriel personnels: Vos obligations en matière d'accès et de protection de la vie privée, juin 2016, **https://www.ipc.on.ca/wp-content/uploads/2016/08/instant-messaging.pdf**

La communication de renseignements personnels sur la santé par courriel, septembre 2016, **https://www.ipc.on.ca/wp-content/uploads/2016/09/fs-health-communicating-phi-by-email-f.pdf**

Protect Against Phishing, juillet 2019, **https://www.ipc.on.ca/wp-content/uploads/2019/07/fs-tech-protect-against-phishing-e.pdf**

Gouvernement fédéral

Commissariat à la protection de la vie privée du Canada, *Blogue savoir techno : Vidéoconférence – Gardez vos distances, et gardez-vous d'exposer vos renseignements personnels*, 1er mai 2020, **https://www.priv.gc.ca/fr/blogue/20200501/**

Alberta

Office of the Information and Privacy Commissioner, *Managing Records When Transitioning from Work to Home*, avril 2020, **https://www.oipc.ab.ca/resources/managing-records-when-transitioning-from-work-to-home-advisory.aspx**

Saskatchewan

Office of the Saskatchewan Information and Privacy Commissioner, *Pandemic Binder: Statements and Blogs by the Saskatchewan IPC during the COVID-19 Pandemic*, **https://oipc.sk.ca/assets/pandemic-binder.pdf** [comprend un billet de blogue sur le télétravail]

Office of the Saskatchewan Information and Privacy Commissioner, *Best Practices for Transporting Personal Information (PI) and Personal Health Information (PHI) Outside of the Office*, avril 2020, **https://oipc.sk.ca/assets/best-practices-for-transporting-pi-phi-outside-the-office.pdf**

Manitoba

Ombudsman du Manitoba, *La protection des renseignements personnels et des renseignements médicaux personnels lors du travail hors du bureau*, **https://www.ombudsman.mb.ca/uploads/document/files/protecting-personal-info-outside-office-fr-fr.pdf**

Québec

Commission d'accès à l'information du Québec, *Sécurité de l'information et télétravail : employeur*, mai 2020, **https://www.cai.gouv.qc.ca/covid-19-questions-frequentes/securite-de-linformation-et-teletravail-employeur/**

Commission d'accès à l'information du Québec, *Sécurité de l'information et télétravail : employé*, mai 2020, **https://www.cai.gouv.qc.ca/covid-19-questions-frequentes/securite-de-linformation-et-teletravail-employe/**

Au sujet du CIPVP

Le rôle du commissaire à l'information et à la protection de la vie privée est décrit dans trois textes de loi : la *Loi sur l'accès à l'information et la protection de la vie privée*, la *Loi sur l'accès à l'information municipale et la protection de la vie privée* et la *Loi sur la protection des renseignements personnels sur la santé*. Le commissaire est nommé par l'Assemblée législative de l'Ontario et est indépendant du gouvernement au pouvoir.

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario