

Travail à distance sécurisé



Présentation et considérations	Considérations techniques	L'utilisation sécuritaire des outils de collaboration	Considérations relatives aux ap
--------------------------------	---------------------------	---	---------------------------------

Qu'est-ce que le travail à distance?

Le travail à distance est lorsqu'un employé peut effectuer des fonctions opérationnelles à partir d'un emplacement éloigné qui se trouve à l'extérieur de l'espace de travail physique de son employeur, habituellement par l'entremise d'Internet. Dans le cadre des événements récents, le travail à distance est devenu plus populaire que jamais, et il continuera à gagner en popularité au fur et à mesure que la technologie évolue.

Obligation de tenir des registres

En vertu de la Directive sur les services et le numérique (<https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32601>), les employés sont tenus de conserver l'information relative à toute activité ou prise de décisions ayant une valeur opérationnelle. Ainsi, que l'activité ou prise de décisions ait eu lieu dans le contexte de l'utilisation d'outils d'informatique en nuage publics ou approuvés par le ministère, l'information doit être consignée (p. ex., dans un document Word) et sauvegardée dès que possible dans un dépôt ministériel tel que GCdocs. Pour obtenir de plus amples renseignements, veuillez cliquer [ici](https://www.canada.ca/fr/gouvernement/fonctionpublique/covid-19/gestion-donnees-gouvernementales-travail-distance.html) (<https://www.canada.ca/fr/gouvernement/fonctionpublique/covid-19/gestion-donnees-gouvernementales-travail-distance.html>).

Le travail à distance et le télétravail

Même s'ils sont semblables et qu'ils sont utilisés de façon interchangeable la plupart du temps, le travail à distance et le télétravail ne sont pas la même chose. Les employés qui télétravaillent et ceux qui travaillent à distance utilisent souvent les mêmes appareils et technologies pour travailler, comme les outils de collaboration, les plateformes d'informatique en nuage et Internet.

Voici les différences entre ces deux options :

Travail à distance	Télétravail
Une situation plus permanente.	Généralement pour une période limitée (jours au lieu de mois ou d'années).
L'employé n'a probablement pas accès à un bureau.	L'employé(e) possède un bureau, mais il/elle travaille à partir d'ailleurs.

Menaces et défis posés par le travail à distance

En se connectant par Internet à des applications ou à des données possiblement classifiées ou sensibles, il est possible que la sécurité des renseignements soit menacée.

Voici certains problèmes liés à la sécurité :

- Manque de sécurité physique – Les appareils peuvent être volés, les lecteurs peuvent être copiés ou des personnes peuvent regarder par-dessus votre épaule.
- Réseaux non sécurisés – La connexion à des réseaux non sécurisés comme dans un café ou un hôtel, ou d'autres réseaux publics ouverts est une cible facile à exploiter.
- Accès interne à l'extérieur – Les serveurs seront confrontés à Internet, ce qui augmentera le risque possible et la vulnérabilité à la compromission.
- Détournement de téléconférence/Zoom – Des personnes non autorisées qui accèdent à une conférence en se joignant à une conférence publique, en communiquant le lien ou le code d'accès.

Mesures de sécurité recommandées

Il est important de se rendre compte que, puisque le travail à distance utilise Internet pour la connectivité, il peut s'agir d'une cible de compromission. Par conséquent, voici certaines mesures utiles que les employés peuvent prendre afin d'assurer la sécurité des renseignements :

Considérations liées aux appareils

- Lorsque l'option d'authentification multifactorielle est disponible, servez-vous en!
- Évitez de vous servir de réseaux ouverts comme dans les cafés, les installations publiques et les hôtels.
- Appliquez les mises à jour du système d'exploitation lorsqu'elles sont disponibles.
- Utilisez le réseau privé virtuel de votre ministère pour avoir une connexion sécurisée.
- Protégez tous les disques durs, les clés USB, et les cartes SD à l'aide d'un mot de passe.
- Verrouillez les appareils lorsque vous ne les utilisez pas.

Considérations liées aux services

Voici quelques éléments généraux dont vous devriez tenir compte quant à l'utilisation de ces applications :

- Activer l'authentification à deux facteurs.
- Afficher ou envoyer des choses qu'il ne vous dérange pas de communiquer à votre employeur ou aux autres employés.
- Séparer les applications personnelles et les applications liées au travail.
- Utiliser des appareils personnels pour des applications personnelles et des appareils de travail pour des applications liées au travail.
- Veiller à ce que les téléconférences soient privées et protégées à l'aide d'un mot de passe.
- Utiliser des outils de collaboration lorsque vous travaillez dans un environnement NON CLASSIFIÉ.

Confidentialité et sécurité des outils de collaboration

Les employés devraient toujours utiliser des outils approuvés par le ministère pour collaborer avec leurs collègues, en commençant par Microsoft Teams (niveau Protégé B si l'emplacement de votre ministère a été accrédité à ce niveau, ou non classifié autrement), puis passer à d'autres outils autorisés OutilsGC ou WebEx. Si ces options ne sont pas disponibles, alors la Politique sur l'utilisation acceptable des dispositifs et des réseaux permet l'utilisation d'outils d'informatique en nuage publics comme Slack, Zoom ou Google Hangouts pour effectuer un travail non classifié uniquement. Toutefois, il faut prendre en compte des problèmes de confidentialité avant d'utiliser ces applications.

Il est important de retenir qu'il ne faut jamais utiliser ces applications pour des travaux classifiés ou de nature délicate. Le Centre canadien de cybersécurité (CCC) a fourni des conseils et des considérations sur l'utilisation d'outils d'informatique en nuage publics pour la vidéoconférence.

Lorsque vous choisissez un outil de collaboration, veuillez tenir compte des facteurs suivants :

- Priorisez des solutions qui n'exigent pas que les participants aient à procéder à l'installation d'un client, sauf lorsqu'il est nécessaire de le faire.
- Choisissez une solution qui vous permet de contrôler la façon dont vos données sont gérées. Certaines plateformes peuvent acheminer des données à l'extérieur du Canada ou stocker des données partagées sur des serveurs qui sont sous leur contrôle.
- Veillez à ce que tous les intervenants qui utilisent le logiciel de collaboration soient au fait, et à l'aise, en ce qui a trait à l'échange de données par le propriétaire du logiciel dans le but de réaliser un profit; par exemple, la vente d'analyses de données à des fins de marketing et de publicité.

Pour obtenir une liste complète des facteurs dont vous devriez tenir compte, veuillez consulter l'avis du CCC.

Voici les paramètres et les fonctionnalités qui peuvent contribuer à la sécurité des téléconférences:

- Désactivez le partage d'écran des invités.
- Exigez la présence de l'hôte.
- Sécurisez la conférence avec un mot de passe.
- Gardez votre ID de réunion personnelle ou vos invitations privées.

Slack

Lorsque vous utilisez une licence payante de l'application, une fonction est déverrouillée afin de permettre au personnel des RH et de la gestion d'archiver TOUTES les séances de clavardage. En plus d'être en mesure d'exporter les discussions de groupe, il est également possible d'exporter les conversations privées qui se tiennent entre vous et un collègue. Il est impossible d'activer cette fonctionnalité dans la licence libre. Il est important de prendre note qu'il y a une limite de stockage des données indépendamment de la licence, y compris après 10 000 messages, dans la version gratuite. Slack conserve également des données telles que les liens, les mots de passe, les noms d'utilisateur et les séances de clavardage, mais dispose d'options pour personnaliser les stratégies de conservation des données.

Voici des paramètres et des fonctionnalités qui peuvent contribuer à la sécurité de Slack :

- Demandez aux membres du groupe d'utiliser l'authentification à deux facteurs (2FA).
- Gérez la capacité d'installer des applications et de connecter des outils à un espace de travail de groupe.
- Limitez l'accès à l'espace de travail.
- Soyez prudent à l'ouverture de liens, surtout si vous ne les avez pas demandés.
- Limitez les fonctions administratives.

Pour obtenir de plus amples renseignements sur l'utilisation de Slack en toute sécurité, veuillez consulter le Centre d'aide Slack.

Zoom

Zoom comprend une fonction qui porte une attention à la caméra Web afin de voir qui est actif dans le cadre de la discussion vidéo. Si un participant partage son écran et qu'un utilisateur réduit la fenêtre ou quitte son appareil, les hôtes de la réunion recevront un avis. Il faut prendre note qu'il n'est pas enregistré pas d'activité sur l'appareil et ne consigne pas de vidéo avec ce paramètre. À la création d'une réunion, Zoom génère un ID aléatoire de neuf à onze chiffres. Pour une personne disposant de ressources informatiques, il peut être facile de décrypter le code, ce qui permet à des acteurs malveillants de se joindre à l'appel. Pour obtenir de plus amples renseignements sur la création d'une conférence Zoom, veuillez consulter la section des références ou cliquez ici.

Pour en apprendre davantage sur les pratiques exemplaires et les fonctions d'accessibilité, veuillez consulter les Pratiques exemplaires d'accès à l'information (EIA) d'ESDC sur l'utilisation de Zoom pour les réunions et les cours (en anglais).

Google Hangouts

Google Hangouts nécessite en effet que l'utilisateur possède un compte Google. Il est préférable d'utiliser un compte de travail si possible pour éviter que des renseignements ne soient reliés les uns aux autres, exposant ainsi les intérêts personnels, de même que votre activité personnelle en ligne lorsqu'il y a un lien avec ce compte Google. Des renseignements tels que les noms, les numéros de téléphone, les noms d'utilisateur et d'autres renseignements peuvent être regroupés et exposés en tant qu'entité unique afin d'exploiter d'autres renseignements et intérêts personnels.

Google stocke les images qui ont été envoyées par l'entremise de Hangouts à une adresse URL publique, ce qui signifie que n'importe qui peut techniquement consulter l'image à condition qu'il possède la bonne adresse URL. Un autre problème avec Hangouts est que cette application n'est pas sécurisée d'un chiffrement de bout en bout. En termes simples, le chiffrement ne se produit qu'à l'envoi. Cela ouvre la porte à l'écoute des discussions ainsi qu'à la visibilité des messages ayant été échangés par l'entremise de Google.

Références

- Problèmes de sécurité liés au télétravail (https://cyber.gc.ca/sites/default/files/publications/itsap.10.016-fra_0.pdf)
- Les réseaux privés virtuels (<https://cyber.gc.ca/sites/default/files/publications/ITSAP.80.101-fr.pdf>)
- Orientation sur la facilitation de l'accès aux services Web - SCT (https://wiki.gccollab.ca/images/4/4e/Orientation_sur_la_facilitation_de_l%E2%80%99c%C3%A8s_aux_services_Web.pdf)
- Bulletin sur le télétravail sécurisé - NIST (<https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2020-03.pdf>)
- Guide sur le télétravail d'entreprise, l'accès à distance - NIST (<https://doi.org/10.6028/NIST.SP.800-46r2>)

Retrieved from "https://wiki.gccollab.ca/index.php?title=T%C3%A9l%C3%A9travail_%C3%A0_distance_s%C3%A9curis%C3%A9&oldid=24910"

This page was last edited on 7 May 2020, at 14:24.

Content is available under [Creative Commons Attribution 4.0 International License](#) unless otherwise noted.