# Conseils pour l'utilisation sécuritaire des outils de collaboration

## CONTEXTE

La Politique sur l'utilisation acceptable des dispositifs et des réseaux (PUADR) du gouvernement du Canada reconnaît que le libre accès aux outils modernes est essentiel pour transformer la façon dont les fonctionnaires travaillent et servent la population canadienne. Cette Politique exige que les fonctionnaires aient un accès ouvert à Internet, notamment aux sites du GC et aux outils et services externes qui amélioreront la communication et la collaboration numérique, et qui encourageront le partage des connaissances et de l'expertise pour appuyer l'innovation.

Les outils de collaboration permettent aux fonctionnaires de maintenir un dialogue interactif avec les collectivités qu'ils servent. On peut notamment citer à titre d'exemple des sites comme Twitter et LinkedIn; des outils de partage de présentations en ligne comme Prezi ou SlideShare, ou encore des plateformes de discussion en temps réel comme Slack.

## CONSIDÉRATIONS

Étant donné que les fonctionnaires travaillent de plus en plus dans un environnement ouvert et accèdent sans cesse à de nouveaux outils, il est important que les représentants du GC fassent en tout temps preuve de bonnes compétences en matière d'alphabétisation numérique ainsi que d'un bon jugement en ligne. En ce qui a trait à la sécurité de la TI, les connexions aux outils et services externes comportent les mêmes risques que les autres connexions à Internet. Toutefois, les ministères devraient tenir compte du fait que l'utilisation de ces sites pourrait nécessiter une certaine forme d'identification de la personne et, par conséquent, faciliter son association à une organisation (p. ex., un ministère ou un organisme du GC). De plus, il existe un risque que des renseignements protégés ou de nature sensible soient intentionnellement ou non exposés au public. Par conséquent, les ministères doivent tenir compte de ce qui suit :

> *La cybersécurité n'est pas l'apanage de ceux qui ont le mot « cybersécurité » dans leur titre de poste. Il incombe à tous de suivre les pratiques exemplaires en matière de cybersécurité.*
>
> ***La sécurité, c'est l'affaire de tous.***

- publier de l'information sur des outils externes et des services Web divulguera probablement l'origine de l'information;
- toute information publiée par l'entremise d'Internet, pour quelque durée que ce soit, est effectivement enregistrée de façon permanente. Il n'existe pas mesure pour contrôler l'information une fois qu'elle est publiée;
- la nature des outils externes et des services Web comme les réseaux sociaux en fait des cibles attrayantes pour les personnes mal intentionnées. Ces sites sont intrinsèquement sujets à la présence

d'utilisateurs peu scrupuleux qui fournissent des liens vers du contenu malveillant susceptible de corrompre l'infrastructure d'un ministère;

- le contenu d'outils externes comme Trello, Slack, etc. peut être stocké sur des serveurs situés à l'extérieur du Canada, de sorte que le contenu et les métadonnées d'utilisateur connexes peuvent être surveillés par des produits, des services ou des entreprises non canadiens et/ou des tierces parties;
- tout ce qui est partagé au moyen d'outils externes et de services Web pourrait être assujetti à la *Loi sur l'accès à l'information et la protection des renseignements personnels* (AIPRP). Les fonctionnaires doivent s'assurer que l'information relative au mandat de l'organisation et/ou contenant des décisions sur les activités gouvernementales est correctement saisie et gérée, conformément aux meilleures pratiques de gestion de l'information;
- on encourage les fonctionnaires à vérifier les exigences en matière de conservation des données lorsqu'ils utilisent des outils externes, conformément à la Politique sur la gestion de l'information du SCT. Certains outils externes conserveront vos données même après la désactivation de votre compte[1].

Les employés sont tous responsables de protéger l'information et les biens qui sont sous leur contrôle, d'appliquer les mesures de sécurité liées aux processus courants, de signaler les incidents de sécurité et de se tenir au fait des enjeux et des questions de sécurité. Ces outils doivent être utilisés pour collaborer et faciliter le travail, et non pas pour remplacer les outils organisationnels auxquels vous avez actuellement accès ni contourner les mesures de sécurité. En faisant chacun notre part pour contribuer à protéger le GC, nous établirons une première ligne de défense plus solide.

## CONSEILS AUX UTILISATEURS

| QUOI FAIRE | ET NE PAS FAIRE |
|---|---|
| • Protéger son identité à l'aide des paramètres de confidentialité de tous les outils et appareils, et limiter la publication de renseignements sur sa page de profil.<br>• Utiliser de solides mécanismes d'authentification (p. ex., l'authentification multifactorielle) dans la mesure du possible pour se prémunir contre l'accès non autorisé et permettre le verrouillage automatique d'un appareil.<br>• Utiliser des systématiquement des mots de passe différents, notamment pour les comptes personnels et professionnels. | • Ne jamais partager de renseignements protégés ou de nature délicate, à moins d'y avoir été expressément autorisé par le groupe de technologie de l'information ministériel.<br>• User de prudence en ouvrant des liens non sollicités ou des pièces jointes, ou lorsqu'on nous demande d'installer un logiciel. Réfléchir avant d'agir si on ne connaît pas l'expéditeur ou qu'on ne s'attendait pas à recevoir un lien ou une pièce jointe.<br>• Ne pas réutiliser les mêmes mots de passe que ceux utilisés pour se connecter à l'interne.<br>• Faire preuve de prudence et éviter d'utiliser des réseaux non fiables ou un réseau Wi-Fi gratuit. |

[1] https://slack.com/privacy-policy

| QUOI FAIRE | ET NE PAS FAIRE |
|---|---|
| • Être conscient de ce que l'on partage et avec qui et partir du principe que tout ce qui est partagé pourrait être rendu public.<br>• Utiliser des systèmes d'exploitation modernes et des navigateurs Web à jour configurés à l'aide des mesures appropriées de protection du système central.<br>• Signaler toute activité suspecte ou tout incident de sécurité afin que l'équipe de sécurité ministérielle puisse régler le problème.<br>• Mettre en œuvre les pratiques exemplaires en matière de GI et sauvegarder les décisions prises à l'aide d'un outil de collaboration dans le répertoire de GI du ministère.<br>• Indiquer clairement dans notre profil de médias sociaux (utilisé à des fins professionnelles) que les opinions qui y sont publiées sont les nôtres et non celles de notre employeur. Ceci ne nous dispense pas de remplir nos obligations ou d'adopter les comportements que l'on est en droit d'attendre d'un fonctionnaire. | • Ne jamais publier ni partager de mots de passe ou d'identifiants dans les services et outils Web.<br>• Ne pas ignorer les erreurs de certificat SSL et les sites Web non sécurisés (p. ex., HTTP) |

## CONSEILS SUPPLÉMENTAIRES

Voici quelques conseils et renseignements sur la façon de vous protéger en ligne :

- Sécurité publique : Activités en ligne – La vie en ligne
- CST : Fiche de conseils

## RÉFÉRENCES

- Politique sur l'utilisation acceptable des dispositifs et des réseaux (PUADR)
- Orientation sur l'habilitation de l'accès aux services Web : Avis de mise en œuvre de la politique
- Politique sur la sécurité du gouvernement
- Directive sur la gestion de la sécurité ministérielle
- Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI)
- La gestion des risques liés à la sécurité de la TI : Une méthode axée sur le cycle de vie
- Les 10 mesures de sécurité des TI du Centre de la sécurité des télécommunications Canada (CSTC)
- CSTC, ITSB-66, Les risques à la cybersécurité associés à l'utilisation de médias sociaux - Conseils à l'intention du gouvernement du Canada

- Politique sur l'accès à l'information
- Politique sur la protection de la vie privée
- Ligne directrice sur l'utilisation acceptable des dispositifs et des réseaux (LDUADR)
- Politique sur la gestion de l'information

## DEMANDES DE RENSEIGNEMENTS

Pour obtenir de plus amples renseignements ou des éclaircissements au sujet de ce document, veuillez communiquer avec le Bureau du dirigeant principal de l'information du SCT, Cybersécurité (zztbscybers@tbs-sct.gc.ca).