Considérations de sécurité matérielle pour les environnements de télétravail et de travail à distance

GSMGC-008 (2022)

Préparé par :
Gendarmerie royale du Canada
Principal organisme responsable de la sécurité matérielle
Sous-direction de la sécurité ministérielle
Direction générale 73, Promenade Leikin, Ottawa (Ontario) K1A 0R2

Date de publication : 2022-XX-XX
Mise à jour :

Avant-propos

Le guide *Considérations de sécurité matérielle pour les environnements de télétravail et de travail à distance* est une publication NON CLASSIFIÉE, diffusée avec l'autorisation du principal organisme responsable de la sécurité matérielle de la Gendarmerie royale du Canada (PORS de la GRC).

Cette publication du gouvernement du Canada sert de guide sur les considérations de sécurité pour les environnements de télétravail et de travail à distance à l'intention des ministères, organismes et employés du gouvernement du Canada.

Les suggestions de modifications et les autres renseignements peuvent être envoyés au principal organisme responsable de la sécurité de la GRC par courriel : RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

Date d'entrée en vigueur

La date d'entrée en vigueur du guide GSMGC-008 (2022) *Considérations de sécurité matérielle pour les environnements de télétravail et de travail à distance* est le 2022-XX-XX.

Registre des modifications

N° de modification	Date	Auteur	Résumé de la modification

Remarque : Le principal organisme responsable de la sécurité matérielle de la Gendarmerie royale du Canada est autorisé à apporter des modifications.

Table des matières

1. Introduction

1.1. But

Le présent guide a pour but de fournir aux employés du gouvernement du Canada (GC) qui travaillent ailleurs que dans leur lieu de travail désigné de l'information sur l'évaluation de la sécurité matérielle et sur l'observation des exigences appropriées en matière de protection et d'entreposage des documents et des biens du GC. Les employés devraient également consulter les guides, procédures, normes, directives et politiques de sécurité de leur ministère pour obtenir de l'information et des consignes supplémentaires.

Le présent guide, en plus d'aborder les menaces accrues qui accompagnent l'accès physique aux renseignements et aux appareils dans un environnement de travail à distance ou de télétravail, procure aux employés du GC des outils pour assurer leur protection ainsi que celle des renseignements, des biens ou des appareils dans ce contexte.

1.2. Applicabilité

Le présent guide décrit les exigences en matière de sécurité matérielle pour les lieux de travail à distance/télétravail, y compris celles qui concernent les biens, renseignements et documents papier de nature délicate. Bien qu'il aborde la sécurité matérielle des appareils électroniques, le guide ne traite pas de la sécurité de la GI-TI (cyber sécurité) des systèmes du GC utilisés aux fins de la création, du traitement ou du stockage d'information sous forme électronique.

Certains ministères et employés du GC peuvent adopter une formule hybride au lieu d'opter pour une formule de travail à distance/télétravail à temps plein. On entend par « formule hybride » le fait, pour un employé, de travailler en partie dans un lieu de travail désigné du GC et en partie dans un lieu de travail à distance/télétravail. Le présent guide porte précisément sur les lieux de travail à distance/télétravail et ne décrit pas les exigences en matière de sécurité qui s'appliquent aux lieux de travail désignés du GC. L'adoption d'une formule hybride plutôt que d'une formule de travail à distance/télétravail à temps plein ne saurait être interprétée comme permettant l'assouplissement ou l'omission des mesures de sécurité exigées dans un lieu de travail à distance/télétravail. Toutes les recommandations énoncées ici devraient tout de même être suivies.

Le présent guide doit servir à soutenir la prise de décisions sur les demandes relatives au travail à distance/télétravail, mais ne doit pas être considéré comme la seule source d'information sur les considérations de sécurité matérielle dans un contexte de travail à distance/télétravail. D'autres guides du PORS de la GRC pourraient s'avérer nécessaires pour évaluer pleinement la sécurité du travail à distance/télétravail. Le cas échéant, vous les trouverez dans la page Web du principal organisme responsable de la sécurité matérielle de la Gendarmerie royale du Canada (rcmp-grc.gc.ca).

1.3. Considérations relatives à la technologie de l'information

En raison des menaces en constante évolution qui nous entourent et de la convergence de la sécurité matérielle et de la sécurité des technologies de l'information, il est crucial d'évaluer le risque associé à l'utilisation des applications et/ou des logiciels connectés à un réseau qui servent à faire fonctionner l'équipement et à le prendre en charge dans les édifices à accès contrôlé du gouvernement du Canada. Quelques exemples de ces applications ou de ces logiciels de commande peuvent comprendre, entre autres, l'éclairage de sécurité, les barrières de périmètre, les portes et le CVCA.

Avant de mettre en place une application et/ou un logiciel pour commander et/ou automatiser certaines fonctions de l'édifice, la sécurité ministérielle demande qu'une Évaluation et autorisation de sécurité (EAS) soit effectuée. Cette EAS garantira le maintien de l'intégrité et de l'accessibilité des composants contrôlés par les applications et/ou les logiciels ainsi que l'atténuation de tout risque mis en évidence. Il est fortement recommandé de commencer le processus d'EAS tôt pour s'assurer du respect de l'échéancier de livraison du projet. Pour plus d'information sur le processus d'EAS, veuillez consulter la sécurité ministérielle.

2. Coordonnées

Pour obtenir de plus amples renseignements, veuillez communiquer avec :

Gendarmerie royale du Canada
Principal organisme responsable de la sécurité matérielle
73, promenade Leikin, arrêt postal 165
Ottawa (Ont.) K1A 0R2
Courriel : RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

3. Sigles

Abréviation/sigle	Signification
DPRH	Dirigeant principal des ressources humaines
DPI	Dirigeant principal de l'information
CST	Centre de la sécurité des télécommunications
DPS	Dirigeant principal de la sécurité
MDN (CNS)	Ministère de la Défense nationale (Centre national spécial)
AMC	Affaires mondiales Canada
GC	Gouvernement du Canada
GI-TI	Gestion de l'information et technologies de l'information
PORS de la GRC	Principal organisme responsable de la sécurité matérielle de la GRC
SPC	Services partagés Canada
SCT	Secrétariat du Conseil du Trésor du Canada
RPV	Réseau privé virtuel

4. Glossaire

Terme	Définition
Travail à distance/télétravail	Dans le présent guide, nous utilisons le terme générique « travail à distance/télétravail » pour désigner toutes les combinaisons de travail à distance ou de télétravail accompli « ailleurs que dans un lieu de travail désigné ».
Travail à distance	Travail accompli dans un endroit différent du lieu de travail désigné. Il s'agit d'un processus mené par l'employeur dans le cadre duquel ce dernier tient compte de la santé et de la sécurité de ses employés. Le recours au travail à distance a généralement lieu dans des circonstances temporaires et imprévisibles : pandémies, états d'urgence, intempéries, etc.
Télétravail	Travail effectué par un employé depuis un endroit différent de son lieu de travail désigné, à la demande de l'employé lui-même, sous réserve des exigences opérationnelles et de l'approbation de la direction.
Formule hybride	Combinaison de travail à distance/télétravail et de travail dans un lieu désigné du GC.
Traitement	Consultation, création, bonification, mise à jour, modification ou utilisation à des fins professionnelles de renseignements du GC.

5. Contexte

Le présent guide assimile le travail à distance et le télétravail et n'établit aucune distinction entre les deux pour ce qui est de l'évaluation de la sécurité matérielle et des mesures de sécurité matérielle exigées. En outre, il convient de noter qu'une formule hybride — où l'employé alterne entre le travail à distance/télétravail et le travail dans un lieu désigné du GC ou un espace de travail partagé du GC — ne réduit pas ni ne modifie les exigences en matière de sécurité matérielle dans le lieu de travail à distance/télétravail.

Dans le passé, le recours au travail à distance a découlé de circonstances imprévues, alors que le télétravail a eu lieu à la demande de l'employé. Le travail à distance/télétravail a gagné en popularité dans les ministères du gouvernement à mesure que la confiance à l'égard des systèmes, des processus et des employés s'est accrue. Le Secrétariat du Conseil du Trésor du Canada ne fait aucune distinction entre le travail à distance et le télétravail et utilise ces termes indifféremment.

5.1. Politiques relatives à la sécurité

Les politiques globales du SCT et les normes propres à un ministère s'appliquent aux employés se trouvant dans un lieu de travail à distance/télétravail, même s'ils exercent leurs activités à l'extérieur d'un lieu de travail physique traditionnel. Le travail à distance/télétravail permet de poursuivre les activités opérationnelles pendant qu'un employé se trouve à l'extérieur d'installations qui appartiennent au gouvernement et sont exploitées par celui-ci. Voici une liste partielle des instruments de politique du SCT sur la sécurité qui s'appliquent lorsqu'on songe à recourir au travail à distance/télétravail :

- Politique sur la sécurité du gouvernement (1er juillet 2019);

- Directive sur la gestion de la sécurité (1er juillet 2019);
- Directive sur le télétravail (avril 2020);
- Lignes directrices sur l'optimisation d'un effectif hybride : Pleins feux sur le télétravail (accessible auprès du SCT).

5.2. Menaces accrues

Le travail à distance/télétravail peut accroître la probabilité de compromission des renseignements de nature délicate d'une organisation. L'information traitée dans un contexte de travail à distance/télétravail peut être exposée à des personnes non autorisées, comme la famille, les amis et d'autres personnes. Cela pourrait amener des auteurs de menace (organisés ou opportunistes) à porter atteinte à l'information par diverses méthodes, dont les suivantes :

- Accès physique à l'information et aux appareils;
- Vol de renseignements ou d'appareils;
- Écoute clandestine de réunions et de conversations téléphoniques;
- Affichage d'aperçus de renseignements ou du contenu d'appareils.

6. Décisions relatives au travail à distance/télétravail

Dans les lieux de travail modernes, l'autorisation du travail à distance/télétravail est en train de devenir la norme. Les enjeux touchant l'amélioration de la santé, l'inclusivité et la pollution sont autant de facteurs qui favorisent le recours à ces formules[1]. Dans bien des cas, les employés du GC travaillent avec des renseignements de nature délicate qui prêtent le flanc à des atteintes à la sécurité matérielle lorsqu'on les traite dans un lieu de travail à distance/télétravail. Afin de réduire la vulnérabilité informatique du travail à distance/télétravail, le PORS de la GRC recommande les mesures suivantes dans le cadre de la gestion ministérielle des risques.

- Les dirigeants principaux de la sécurité (DPS) devraient soutenir les gestionnaires ministériels afin de veiller à ce qu'ils prennent des décisions éclairées à l'égard du travail à distance/télétravail.
- Les DPS, les gestionnaires, les superviseurs et les employés devraient déployer tous les efforts possibles pour promouvoir et recommander l'adoption de pratiques évitant ou limitant l'utilisation de documents papier en situation de travail à distance/télétravail, dans la mesure du possible.
- Les DPS et les gestionnaires ainsi que les groupes des RH ministériels ont le pouvoir de décider si le poste d'un employé peut être désigné admissible au travail à distance/télétravail; les employés ne devraient pas pouvoir prendre une telle décision unilatéralement, car certains postes ne se prêtent peut-être pas au travail à distance/télétravail en raison des exigences du poste ou d'autres préoccupations liées à la sécurité.

[1] Directive sur le télétravail du SCT.

6.1. Limites du travail à distance/télétravail

Selon les politiques du SCT, toutes les personnes ayant accès à des renseignements protégés et classifiés doivent avoir la cote ou l'habilitation de sécurité appropriée ainsi que le besoin de savoir. On recommande que les renseignements cotés Protégé C, Secret ou Très secret soient traités seulement dans les zones appropriées d'un lieu de travail désigné du GC. Il faut éviter de traiter ces renseignements dans un lieu de travail à distance/télétravail. (Signalons ici que les renseignements TS ISC NE PEUVENT être traités dans un environnement de travail à distance/télétravail. Le CST et le CNS du MDN sont les seules autorités pouvant accréditer des endroits où l'on peut traiter et entreposer ces renseignements et en discuter.) C'est particulièrement pertinent dans le cas des renseignements sur support papier, où il n'est peut-être pas possible de respecter les exigences en matière d'entreposage. Les DPS — ou des membres supérieurs de la direction, jusqu'à l'administrateur général — sont responsables de la gestion des risques liés aux autorisations accordées aux employés relativement au traitement et à l'entreposage de toutes les catégories de renseignements sur support papier au lieu de travail à distance/télétravail.

6.1.1. Niveaux Protégé A et B

On peut traiter et entreposer ces documents dans un lieu de travail à distance/télétravail situé à l'extérieur d'un lieu désigné du GC lorsque les mesures de sécurité matérielle recommandées dans le présent guide sont en place.

6.1.2. Niveaux Confidentiel et Secret

Le PORS de la GRC recommande un contrôle serré de toutes les demandes relatives au travail à distance/télétravail où des documents cotés Secret pourraient être ou seront traités. Le traitement de documents papier de cette catégorie dans un lieu de travail à distance/télétravail est déconseillé et doit être évité dans la mesure du possible. La manipulation de documents cotés Confidentiel ou Secret durant le transport vers un lieu de travail à distance/télétravail ou durant le traitement à cet endroit devrait être considérée comme présentant un risque plus élevé. Les DPS sont responsables de la gestion des risques liés à ces décisions et devraient confirmer individuellement chaque demande dans cette catégorie afin de s'assurer que toutes les mesures de sécurité exigées sont en place.

6.1.3. Niveaux Protégé C et Très Secret

La manipulation de documents cotés Protégé C ou Très secret durant le transport vers un lieu de travail à distance/télétravail ou durant le traitement à cet endroit devrait être considérée comme présentant un risque inacceptable. Les DPS sont responsables de la gestion des risques liés à ces décisions et devraient confirmer individuellement chaque demande dans cette catégorie tout en examinant toutes les solutions de rechange possibles au travail à distance/télétravail. En l'absence de solutions de rechange, les DPS devraient s'assurer que toutes les mesures de sécurité exigées à l'égard de zones de haute sécurité sont en place, y compris une évaluation de la menace et des risques (EMR) complète. Le PORS de la GRC ne recommande pas l'approbation de demandes relatives au travail à distance/télétravail concernant des personnes qui seront appelées à traiter des documents cotés Protégé C ou Très secret.

6.2. Responsabilités de la direction

Les ministères doivent évaluer toutes les situations de travail à distance/télétravail et gérer les risques liés aux solutions de travail tout en tenant compte des politiques du SCT, des documents d'orientation produits par le PORS de la GRC et des directives et procédures organisationnelles. Le DPS ou son délégué peut accorder l'approbation à une personne, à un groupe, à un service ou à un organisme, selon la procédure de gestion des risques et la tolérance au risque de l'organisation. Dans certains cas, l'approbation peut avoir lieu à l'échelon de l'administrateur général ou à un niveau supérieur de la direction. Il faut tenir compte de l'emplacement du lieu de travail à distance/télétravail proposé. Il ne devrait pas se trouver dans un secteur dangereux de la ville où le taux de criminalité est élevé.

Les gestionnaires devraient informer les employés de leur responsabilité de prendre toutes les mesures de sécurité raisonnables pour protéger les renseignements et les biens de nature délicate du gouvernement contre la divulgation non autorisée, la perte, le vol, l'incendie, la destruction, les dommages ou les modifications. Les gestionnaires devraient rappeler aux employés de suivre les politiques du GC et du ministère et les politiques de sécurité régissant l'utilisation d'appareils électroniques.

On recommande que des systèmes sans papier soient utilisés dans la mesure du possible et que les documents originaux (le cas échéant) soient conservés dans le lieu de travail. Lorsque des documents papier sont requis, on recommande que des copies soient créées pour le transport au lieu de travail à distance/télétravail pour que les originaux restent dans le lieu de travail désigné du GC. Il est recommandé de remplir une fiche de suivi pour tous les documents cotés Secret, Très secret et Protégé C sortis du lieu de travail désigné du GC afin qu'on puisse suivre tous les dossiers et assurer leur intégrité. Les gestionnaires et les employés devraient signer un registre dès qu'ils sortent ou rapportent un dossier et en indiquer le sujet et le nombre de pages.

Il faut passer en revue les ententes de travail à distance/télétravail au moins une fois par année pour s'assurer qu'il n'y a pas eu de changement à l'égard du lieu ou de la situation de travail à distance/télétravail. Les ministères devraient aussi consigner à l'égard de chaque employé en travail à distance/télétravail les renseignements ci-dessous à des fins de suivi :

- son nom;
- son lieu de travail;
- l'équipement et les biens ministériels sous sa responsabilité;
- les registres de renseignements apportés au lieu de travail à distance/télétravail, s'il y a lieu.

6.3. Responsabilités des employés

Les employés qui exercent leurs activités dans un lieu de travail à distance/télétravail doivent respecter toutes les exigences en matière de contrôle de sécurité touchant la possession, la manipulation, le traitement, l'entreposage, le transport, la destruction et la garde des renseignements et des biens du GC et utiliser uniquement les appareils électroniques approuvés à cette fin.

Les employés doivent bien comprendre et appliquer toutes les mesures de sécurité visant le lieu de travail à distance/télétravail qui contribuent au traitement sûr des renseignements du GC à cet endroit. Les employés devraient faire ce qui suit :

- Respecter toutes les politiques et procédures relatives à l'utilisation acceptable des appareils de l'organisation et à la gestion des renseignements organisationnels, ce qui pourrait comprendre la page Web Gestion efficace et sécuritaire des données gouvernementales dans le contexte du travail à distance – Canada.ca.
- Respecter toutes les politiques de sécurité du ministère et du GC touchant des aspects de la protection des renseignements et des biens comme les suivants :
    - le transport, l'entreposage et la destruction des documents et autres biens;
    - la prévention de la divulgation sans autorisation de renseignements durant le traitement, y compris au cours de discussions;
    - l'évitement des discussions relatives à des renseignements protégés ou classifiés sur des appareils non approuvés, au cours de discussions téléphoniques en mode « mains libres » ou en présence de cohabitants;
    - l'utilisation de tout l'équipement fourni (p. ex. : casque d'écoute, contenants sécuritaires);
    - l'aménagement du poste de travail loin des fenêtres, de façon à prévenir la consultation sans autorisation de l'information qui s'affiche à l'écran de l'ordinateur;
    - la déconnexion d'appareils d'assistance virtuels (p. ex. : Google Home, Alexa) afin de prévenir l'enregistrement de conversations professionnelles par ces services;
    - le signalement de tout incident de sécurité, comme la perte de renseignements ou le vol d'appareils électroniques.
- S'assurer de savoir à qui s'adresser si des problèmes susceptibles de miner la sécurité de documents de nature délicate surviennent, surtout s'il s'agit de problèmes en matière de sécurité ou si des appareils ou des renseignements ont été perdus ou volés.
- Suivre toutes les formations obligatoires sur les problèmes en matière de sécurité et les pratiques exemplaires connexes, comme le fait de prêter attention à son entourage, la protection des renseignements et l'entreposage.
- Suivre la procédure ministérielle applicable au stockage de renseignements dans des répertoires organisationnels.
- Suivre les exigences et les procédures touchant la protection électronique des appareils, comme l'activation de l'authentification multifactorielle.
- Adopter les pratiques exemplaires touchant la protection physique des appareils, comme le fait de ne jamais laisser ses appareils sans surveillance en public.
- Comprendre leurs responsabilités pour ce qui est de maintenir l'état/l'utilisabilité du poste de travail à distance/télétravail (services publics, Internet haute vitesse et assurance).

6.4. Équipement de sécurité

Chaque ministère devrait élaborer des procédures pour soutenir et promouvoir l'utilisation d'équipement de sécurité et d'appareils électroniques approuvés dans un lieu de travail à distance/télétravail, en fonction de la catégorie des renseignements traités. L'utilisation de cet équipement devrait aider les employés à protéger les renseignements et les biens durant le transport et dans l'environnement de travail à distance/télétravail et favoriser la sécurité des renseignements et des appareils électroniques. L'équipement de sécurité peut comprendre ce qui suit : sacs de transport sécuritaires, armoires de rangement, casques d'écoute et filtres de confidentialité. Il faut fournir aux employés de l'équipement qui soutient et favorise la sécurité du traitement, de l'entreposage et du transport des renseignements du GC.

Les ministères devraient établir à l'intention des employés des procédures et des systèmes permettant d'accéder à des options d'approvisionnement, de fourniture et de livraison d'équipement de traitement et de sécurité adéquat.

6.5. Travail à distance/télétravail à l'étranger

Le PORS de la GRC déconseille l'approbation de demandes relatives au travail à distance/télétravail à partir de lieux à l'extérieur du pays, car les facteurs à envisager à cette fin sont très complexes. Voir la section 8 du présent guide pour de plus amples renseignements sur les demandes relatives au travail à distance/télétravail à l'étranger.

7. Exigences touchant l'entreposage – Généralités

Il faut déployer tous les efforts possibles pour limiter le besoin de traiter ou d'entreposer des documents papier (peu importe leur catégorie) à l'extérieur de locaux contrôlés par le GC. Les ministères devraient fournir des outils technologiques électroniques et en promouvoir l'utilisation afin d'améliorer la fonctionnalité des postes de travail et de réduire la dépendance envers les documents papier.

Tous les documents papier et les biens — qu'ils se trouvent dans un lieu de travail à distance/télétravail ou dans les locaux du GC — devraient être entreposés conformément aux directives du PORS de la GRC et aux pratiques de sécurité établies par le ministère. Lorsque le matériel n'est pas utilisé ou que l'employé quitte le lieu de travail à distance/télétravail, l'employé devrait :

- effectuer une vérification sommaire pour s'assurer que les fenêtres et les portes sont fermées et verrouillées;
- s'assurer que tous les documents sont entreposés conformément aux directives du PORS de la GRC et aux procédures et politiques du ministère;
- déconnecter les appareils électroniques des réseaux, systèmes et RPV, puis les éteindre;
- conformément à la catégorie des renseignements ou des biens, utiliser les contenants sécuritaires appropriés pour ranger sécuritairement et séparément l'équipement électronique, les cartes/jetons ICP ou autres appareils lorsqu'il s'absente du lieu de travail à distance/télétravail;
- fermer les stores ou autres couvre-fenêtre de la zone de travail (le cas échéant);

- mettre en service le système d'alarme (le cas échéant);
- si une absence prolongée du lieu de travail à distance/télétravail est prévue (p. ex. pour les vacances), songer à retourner les renseignements et les biens au lieu désigné du GC pour qu'ils soient gardés en lieu sûr. À tout le moins, l'employé devrait aviser son gestionnaire des mesures d'entreposage prises au lieu de travail à distance/télétravail.

7.1. Exigences d'entreposage – niveaux Protégé A et B

Entreposage

Il faut conserver les documents cotés Protégé A ou B dans un contenant verrouillable. À tout le moins, les renseignements de niveau Protégé B ou plus bas au lieu de travail à distance/télétravail devraient être tenus à l'abri des regards et de tout accès non autorisé lorsqu'ils ne servent pas.

Pièces/bureaux

L'utilisation de mesures de contrôle d'accès devrait être envisagée en vue d'empêcher la consultation ou l'accès sans autorisation.

7.2. Exigences d'entreposage – niveaux Confidentiel et Secret

La GRC ne recommande pas le travail à distance/télétravail touchant des renseignements ou des biens de niveau Confidentiel ou Secret. Lorsque le travail à distance/télétravail touchant de tels renseignements ou biens ne peut être évité, les directives suivantes devraient s'appliquer :

Entreposage

Tous les documents et biens portant l'indication Confidentiel ou Secret devraient être rangés dans des contenants approuvés, conformément au Guide d'équipement de sécurité (GRC G1-001). Les contenants sécuritaires approuvés renfermant des renseignements de niveau Secret devraient être fixés à la structure du bâtiment pour qu'on ne puisse pas les emporter facilement.

Pièces/bureaux

Il faut traiter et entreposer les renseignements de niveau Confidentiel ou Secret dans une pièce réservée pouvant être fermée à clé afin d'empêcher des personnes non autorisées de voir ces renseignements ou d'y accéder. La porte de la pièce devrait être verrouillée à l'aide d'équipement de qualité commerciale lorsqu'il n'y a personne sur place. Il ne faut pas ranger les effets et biens de valeur dans le même contenant que d'autres renseignements ou biens.

Surveillance

Dans le cas d'un lieu de travail à distance/télétravail où l'on traite ou entrepose du matériel de niveau Confidentiel ou Secret, le PORS de la GRC recommande l'installation d'un système d'alarme résidentiel qui est relié à une centrale et peut déclencher une intervention. Le système d'alarme de la pièce où se trouvent les renseignements devrait être doté à tout le moins de contacts de porte et de fenêtre et de détecteurs de mouvement.

7.3. Exigences d'entreposage – niveaux Protégé C et Très secret

Le traitement et l'entreposage de renseignements de niveau Protégé C ou Très secret à l'extérieur des installations approuvées du GC sont considérés comme extrêmement risqués et sont donc déconseillés par le PORS de la GRC. En l'absence de solutions de rechange, le service ministériel responsable de la sécurité matérielle devrait réaliser une évaluation complète de la sécurité du lieu proposé, y compris une EMR. Tous les contrôles de sécurité exigés pour les zones de sécurité de haut niveau des installations du GC devraient servir de norme minimale pour l'aménagement du site.

8. Travail à distance/télétravail à l'étranger

De nombreux ministères du GC ont des employés affectés à l'étranger dans le cadre de leurs fonctions opérationnelles courantes. Le présent guide n'a pas pour but d'influer sur des postes déjà assignés, comme ceux de personnes rattachées aux ambassades et aux hauts-commissariats canadiens. En tant que PORS investi de responsabilités touchant l'exercice du leadership ainsi que la fourniture de conseils et de directives à l'égard de la sécurité dans les missions à l'étranger, Affaires mondiales Canada (AMC) serait peut-être une bonne source d'information si des ministères décident d'approuver des demandes relatives au travail à distance/télétravail à l'étranger.

Le PORS de la GRC ne recommande pas d'autoriser le travail à distance/télétravail à partir de lieux à l'extérieur du pays. Il convient de signaler aux ministères que toute demande relative au travail à distance/télétravail international requiert une évaluation de sécurité et un processus d'approbation très intensifs ainsi qu'une évaluation des considérations touchant l'administration et l'immigration pour veiller à ce que toute exigence pertinente soit cernée. Les ministères susceptibles d'autoriser le travail à distance/télétravail à l'étranger devraient élaborer un processus prévoyant des contrôles de sécurité complets, des évaluations des risques, des approbations et des séances d'information.

8.1. Directives du SCT

Selon les Lignes directrices sur l'optimisation d'un effectif hybride du SCT, le recours au travail à distance/télétravail à l'étranger ne devrait pas être la norme. On s'attend à ce que les employés travaillent à partir du Canada, à moins d'être appelés à exercer leurs fonctions courantes à l'étranger. Les demandes relatives au travail à l'extérieur du Canada ne devraient être approuvées que dans des circonstances exceptionnelles, à la lumière d'un examen par le DPS, les spécialistes fonctionnels de la sécurité, le chef des Ressources humaines de l'organisation et les spécialistes des ressources humaines. Les approbations ministérielles à l'égard de la demande devront provenir d'un échelon de direction supérieur (pouvant aller jusqu'à l'administrateur général) à ce que prévoit la procédure normale liée au télétravail au pays. Les risques associés au travail à l'extérieur du Canada pourraient avoir de graves implications sur des aspects ne touchant pas la sécurité, comme les exigences liées au visa d'emploi et à l'impôt, l'accès aux soins de santé et aux prestations d'assurance maladie, la santé publique et l'intervention d'urgence, et les relations diplomatiques. La capacité des ministères d'exercer adéquatement leur devoir de vigilance envers leurs employés pourrait être limitée à l'étranger.

Les demandes relatives au travail à distance/télétravail international devraient :

- n'être envisagées que dans des circonstances exceptionnelles;
- être limitées à une période précisée;
- faire l'objet d'un examen administratif approfondi;
- faire obligatoirement l'objet une EMR complète à l'égard de l'employé, du pays et de la ville où le travail sera accompli;
- nécessiter l'approbation supplémentaire ou spéciale des personnes suivantes :
    - administrateur général;
    - DPS du ministère;
    - DPRH du ministère;
    - DPI du ministère;
    - Services partagés Canada (exiger la permission de SPC d'utiliser tout appareil du GC connecté à un réseau Internet international qui se connecte aux réseaux du GC).

8.2. Sécurité personnelle (à l'étranger)

En plus des implications décrites plus haut, le travail à distance/télétravail international présente des risques de sécurité accrus pour la personne intéressée et le GC. La Convention de Vienne sur les relations diplomatiques (1963) ne s'appliquerait pas aux employés du GC travaillant à l'étranger qui ne sont ni des membres du personnel diplomatique ni des personnes à charge d'un membre du personnel. Ces employés seront assujettis à toutes les lois locales et d'État et ne jouiront d'aucune protection diplomatique touchant les renseignements, les biens ou la propriété, y compris les renseignements et les biens du GC. Dans certains pays, l'employé du GC pourrait avoir des problèmes du fait qu'il travaille au nom d'un gouvernement étranger sur le territoire du pays d'accueil.

Les responsabilités liées au devoir de vigilance des employeurs pourraient être limitées à l'étranger lorsque surviennent des événements météorologiques extrêmes, des révoltes armées ou d'autres événements du genre. Les responsables ministériels devraient être conscients de la possibilité de tels problèmes pour les employés travaillant à l'étranger avant d'approuver des demandes. Les employés qui demandent à faire du travail à distance/télétravail international devraient aussi être informés de ces limites.

Les notions fondamentales de sécurité personnelle que tous les Canadiens tiennent pour acquises n'existent peut-être pas à l'endroit où l'employé veut aller. Les taux de criminalité élevés, l'accès limité à la police ou aux services de sécurité et l'existence de services de collecte de renseignements perfectionnés font partie de la réalité de nombreux pays, ce qui soulève des préoccupations à l'égard de la sécurité de l'employé, de sa famille et de sa résidence. Il faut soupeser l'ensemble des données probantes à la lumière des avantages avant d'approuver une demande relative au travail à distance/télétravail à l'étranger.

8.3. Sécurité matérielle (à l'étranger)

En plus des implications décrites plus haut, le travail à distance/télétravail international présente des risques de sécurité matérielle accrus. Les employés qui travaillent à l'étranger sans protection diplomatique sont assujettis à toutes les lois locales et d'État et exposés à la

situation en matière de sécurité dans le pays où ils choisissent de travailler. La criminalité (y compris les crimes contre la personne ou les biens et les crimes intellectuels), l'intervention policière limitée, la pauvreté, les catastrophes naturelles, les activités parrainées par l'État et les tendances xénophobes sont autant d'aspects pouvant caractériser la situation en matière de sécurité de la destination internationale. Les mesures de sécurité matérielle à certains endroits pourraient s'accompagner de coûts prohibitifs ou être difficiles à maintenir en l'absence de ressources de sécurité ministérielle. En tant que principal organisme responsable de la sécurité, AMC pourrait être en mesure de contribuer à la fourniture de conseils sur les mesures de sécurité à prendre pour protéger le personnel, les renseignements et les biens du GC.

La portée et la conduite d'une enquête sur la sécurité internationale ou d'une EMR vont au-delà des paramètres du présent guide, et il convient de rappeler à nouveau que le PORS de la GRC ne recommande pas l'approbation de demandes relatives au travail à distance/télétravail international. Avant d'approuver une telle demande, le ministère doit tenir compte de sa capacité de mettre en œuvre et de maintenir les mesures et contrôles de sécurité qui s'imposent.

Voici une liste de mesures de sécurité pouvant s'avérer nécessaires pour protéger le personnel, les renseignements et les biens du GC à l'étranger, selon la situation en matière de sécurité propre au lieu en question. Il ne s'agit pas d'une liste exhaustive, car les besoins dépendent fortement du lieu :

- Emplacement – le lieu de travail à distance/télétravail ne devrait pas se trouver dans un secteur dangereux de la ville/du pays où le taux de criminalité est élevé.
- Aménagement de clôtures de sécurité, de murs ou de barrières autour du site, y compris un dispositif anti-escalade.
- Installation d'un système de caméras en circuit fermé permettant l'enregistrement et le visionnement.
- Installation d'un système de sécurité et d'alarme résidentiel offrant une capacité d'intervention fiable.
- Embauche de gardiens de sécurité résidentielle.
- Installation de dispositifs de verrouillage de sécurité robustes sur l'ensemble des fenêtres, portes, barrières, etc.
- Utilisation de pellicules de protection, de barres ou de grillages sur les fenêtres.
- Installation de barrières, de grillages ou de grilles extensibles.
- Aménagement de zones sûres ou de pièces de survie dans la résidence.
- Accès à des contenants de sécurité matérielle approuvés et utilisation de ceux-ci pour protéger les renseignements et les biens.
- Capacités et coordonnées des intervenants d'urgence locaux (police, pompiers, ambulance, etc.).
- Confirmation de l'existence de mécanismes de soutien consulaire adéquats de l'ambassade ou du haut-commissariat.
- Mise en place de mesures de sécurité appropriées à l'égard de la TI (conformément aux exigences de SPC et du CST).
- Établissement de plans d'évacuation et accès aux coordonnées de personnes-ressources dans des tiers pays sûrs.

- Tenue de séances d'information et fourniture de formations propres au pays à l'intention des membres du personnel en télétravail à l'étranger.

9. Autres considérations de sécurité

9.1. Formation sur la sensibilisation à la sécurité

On recommande que les ministères élaborent et fournissent à chaque employé (individuellement ou en groupe) une formation de sensibilisation à la sécurité en tant que condition d'approbation des demandes relatives au travail à distance/télétravail. Il serait peut-être judicieux d'offrir périodiquement des séances d'information sur la sécurité et des formations d'appoint.

9.2. Cohabitation

Tous les employés doivent détenir une cote de sécurité valide; cette exigence pourrait, dans des circonstances exceptionnelles, être envisagée pour les cohabitants. La décision d'imposer cette exigence serait laissée à la discrétion du DPS ou d'un membre supérieur de la direction lorsque l'employé en travail à distance/télétravail serait appelé à traiter des renseignements de niveau Secret ou plus. Les employés devraient signaler les changements touchant la cohabitation ou tout autre facteur susceptible d'influer sur la posture de sécurité du lieu de travail à distance/télétravail ou sur l'habilitation de sécurité/le statut des employés.

9.3. Expiration de l'habilitation ou de la cote de sécurité

Les gestionnaires devraient systématiquement vérifier l'habilitation ou la cote de sécurité des employés et indiquer celles qui expireront durant la période de travail à distance/télétravail.

9.4. Transport

Les renseignements et les biens de nature délicate devraient être transportés conformément au guide GSMGC-007 Transport, transmission et entreposage de renseignements protégés ou classifiés et aux procédures ministérielles connexes. Les employés devraient éviter les arrêts inutiles durant le transport de renseignements ou de biens et ne jamais laisser des renseignements ou biens de nature délicate sans surveillance.

9.5. Contrôle de l'information et des biens durant le traitement

Les employés devraient suivre les procédures de base afin de protéger les renseignements de nature délicate durant le travail à distance/télétravail. Ils devraient toujours travailler dans un espace réservé à cette fin, à l'abri du regard des cohabitants ou d'autres personnes (par la fenêtre), et faire tout leur possible pour veiller à ce qu'on ne puisse entendre leurs conversations.

Les employés doivent éviter les discussions relatives à des renseignements protégés ou classifiés sur des appareils non approuvés, lors de discussions téléphoniques en mode « mains libres » ou en présence de cohabitants. L'accès aux renseignements et aux appareils électroniques devrait être bloqué grâce au verrouillage de l'écran d'ordinateur et au rangement de tous les documents papier dans un contenant adéquat.

9.6. Protection et utilisation de supports de stockage électroniques

Les exigences en matière de TI du GC et des ministères ne permettent pas d'utiliser des clés USB ou d'autres mémoires de masse pour le stockage de renseignements protégés ou classifiés du GC ni de connecter des tels dispositifs aux ordinateurs et réseaux du GC. On peut stocker les renseignements et les fichiers à l'aide de dispositifs chiffrés fournis par le gouvernement qui ont été évalués et approuvés par la section de la Sécurité de la TI du ministère. Lorsqu'elles ne sont pas utilisées, les clés USB et les mémoires de masse devraient être entreposées dans des contenants appropriés, selon leur niveau de sécurité. Les ministères et les organismes devraient établir à l'intention de leurs employés des lignes directrices claires sur l'utilisation appropriée de périphériques USB.

9.7. Impression, copie et numérisation

La connexion de périphériques personnels (p. ex. : imprimante, numériseur) aux postes de travail du GC n'est pas permissible. Sous réserve de circonstances opérationnelles exceptionnelles, les employés peuvent demander à utiliser des appareils multifonction au lieu de travail à distance/télétravail. L'impression se fait au moyen d'appareils fournis par le ministère; la numérisation ou la copie de renseignements du GC est déconseillée. Toutes les imprimantes fournies par le ministère devraient lui être retournées lorsqu'elles ne sont plus requises. Les demandes relatives à la capacité d'impression devraient être soumises par le gestionnaire de l'employé, puis examinées et approuvées par le DPS et le programme de Sécurité de la TI du ministère.

9.8. Élimination de renseignements et de biens

Les renseignements et biens protégés et classifiés voués à la destruction devraient être traités de la même manière que tous les autres renseignements et biens. On peut les entreposer de façon sécuritaire au lieu de travail à distance/télétravail en attendant leur retour au lieu de travail du GC en vue de leur destruction/déchiquetage. Le matériel voué à la destruction devrait être transporté conformément au guide GSMGC-007 Transport, transmission et entreposage de renseignements protégés ou classifiés.

9.9. Retour des biens

Les supports et l'équipement de TI fournis par le gouvernement qui ne servent plus devraient être entreposés de façon sécuritaire au lieu de travail à distance/télétravail en attendant leur retour au lieu de travail du GC. Le matériel devrait être transporté conformément au guide GSMGC-007 Transport, transmission et entreposage de renseignements protégés ou classifiés.

9.10. Listes de vérification, guides et schémas de processus

Les ministères devraient élaborer à l'intention des gestionnaires et des employés des listes de vérification ou des schémas de processus à suivre pour s'assurer que les contrôles de sécurité appropriés et d'autres mesures sont utilisés pour atténuer les risques. On peut adapter les listes de vérification aux besoins du ministère et prévoir diverses exigences, dont les suivantes :

- les employés ont une habilitation ou cote de sécurité appropriée et ont besoin de

savoir;
- les employés ont terminé la formation de sensibilisation à la sécurité;
- les employés ont été informés de la procédure à suivre pour protéger les renseignements dans un lieu de travail à distance/télétravail;
- des contrôles de sécurité appropriés sont en place.

L'outil du Centre d'excellence en sécurité pour la prise de décisions sur le travail à distance/télétravail est un bon point de départ au moment d'élaborer une procédure touchant le traitement des demandes relatives au travail à distance/télétravail. Il se trouve sur la page du CEeS, mais il faut avoir un compte GCCollab et appartenir au groupe pour accéder à la trousse d'outils et l'utiliser.

Les ministères et organismes devraient élaborer des guides simples et efficaces pour le travail à distance/télétravail qui serviront d'aide-mémoire sur les pratiques de sécurité recommandées ou déconseillées et rappelleront aux employés leurs responsabilités lorsque leur demande relative au travail à distance/télétravail est approuvée.

10. Références ou documents connexes

- CST, CCC, « Conseils de sécurité pour les organisations dont les employés travaillent à distance » (ITSAP.10.016), mai 2020
- ARC, « Managing Paper Documents in the Home Workspace » (gestion des documents papier dans le lieu de travail), 2020
- Gestion efficace et sécuritaire des données gouvernementales dans le contexte du travail à distance – Canada.ca
- SCT, « Directive sur le télétravail », avril 2020
- GC, « Maladie à coronavirus (COVID-19) : Travail à distance », janvier 2021
- Politique sur la sécurité du gouvernement, 1er juillet 2019)
- Directive sur la gestion de la sécurité, 1er juillet 2019
- Directive sur la gestion de la sécurité – Annexe J : Norme sur la catégorisation de sécurité, 1er juillet 2019
- Directive sur la gestion de la sécurité – Annexe B : Procédures obligatoires relatives aux mesures de sécurité de la technologie de l'information
- GSMGC-007 Transport, transmission et entreposage de renseignements protégés ou classifiés (actuellement G1-009)
- GRC G1-001 – Guide d'équipement de sécurité
- SCT, « Lignes directrices sur l'optimisation d'un effectif hybride : Pleins feux sur le télétravail »

Publication

Examiné et recommandé aux fins d'approbation.

J'ai examiné et je recommande aux fins d'approbation le guide GSMGC-008 (2022) – Considérations de sécurité matérielle pour les environnements de télétravail et de travail à distance.

Nattress,Shawn Thomas,000302786 Digitally signed by Nattress,Shawn Thomas,000302786 Date: 2022.05.10 13:56:07 -04'00'

Shawn Nattress, Date
Gestionnaire
Principal organisme responsable de la sécurité de la GRC

Approuvé

J'approuve par la présente le guide GSMGC-008 (2022) – Considérations de sécurité matérielle pour les environnements de télétravail et de travail à distance.

St-Pierre,Andre Vincent,000171484 Digitally signed by St-Pierre,Andre Vincent,000171484 Date: 2022.05.11 14:30:39 -04'00'

André St-Pierre, Date
Directeur, Sécurité matérielle
Gendarmerie royale du Canada