



2727 COWORKING / RECHERCHE ET CONSEILS PRATIQUES

Sécurité du télétravail : liste pour les petites entreprises au Canada

Find a practical home for your work at 2727 Coworking in Montreal. Explore private offices, day workspaces and meeting rooms, plus business-address and virtual-mailbox services for your company.

Publié par 2727 Coworking · 2026-10-01 · liste-verification-securite-teletravail · cybersecurite-petites-entreprises · canada · securite-wifi-public · cybersecurite-coworking · securite-bureau-domicile · utilisation-appareils-personnels · authentication-multifacteur · donnees-clients

Article original : <https://2727coworking.com/articles/fr/securite-teletravail-liste-petites-entreprises-canada>

Dans cet article

1. Résumé
2. Introduction et contexte
3. Bureau à domicile
4. Café et espace public
5. Espace de coworking
6. Site client
7. Comparaison des caractéristiques
8. Performance et critères de référence
9. Analyse des données et éléments probants
10. Implications et orientations futures
11. Foire aux questions (FAQ)
12. Conclusion

Résumé

Une liste de vérification canadienne pour la sécurité du télétravail commence par la **tâche**, puis passe à l'**appareil**, à la **connexion**, à l'**environnement** et à la **personne à joindre en cas d'incident**. Un bureau à domicile peut convenir au travail confidentiel lorsque le réseau du ménage et l'espace physique sont contrôlés ; un café convient généralement mieux aux tâches portant sur des renseignements publics ou peu sensibles ; un poste en coworking dépend des mesures de contrôle du travailleur et des réponses de l'établissement ; un site client exige le respect des règles d'accès du client. Il s'agit d'un cadre décisionnel rédactionnel, et non d'une certification de quelque lieu que ce soit. Le Centre canadien pour la cybersécurité recommande

d'utiliser, dans la mesure du possible, des appareils appartenant à l'organisation, d'effectuer des mises à jour automatiques et des sauvegardes, et de limiter l'accès selon les besoins du poste. (www.cyber.gc.ca) (www.cyber.gc.ca) (www.cyber.gc.ca)

Le Wi-Fi public présente un risque conditionnel, ce qui ne signifie pas que toute session est dangereuse. La Federal Trade Commission des États-Unis souligne que le chiffrement généralisé des sites Web améliore la sécurité de la navigation Web courante, tandis que le Centre canadien pour la cybersécurité conseille d'éviter, dans la mesure du possible, le Wi-Fi public pour les activités professionnelles. Une connexion cellulaire ou un réseau connu peut réduire l'exposition ; un réseau privé virtuel (VPN) aide uniquement pour le trafic qui y transite et ne peut pas empêcher un utilisateur d'ouvrir un lien malveillant. Confirmez le nom du réseau de l'établissement auprès du personnel et gardez les écrans et les appels confidentiels à l'abri des regards et des oreilles indiscrets. (consumer.ftc.gov) (www.cyber.gc.ca) (www.cyber.gc.ca) (www.ncsc.gov.uk) (www.cyber.gc.ca) (www.getcybersafe.gc.ca)

Les mesures minimales à mettre en place sont des comptes nominatifs, l'authentification multifacteur (MFA), des appareils pris en charge et à jour, le chiffrement intégral du disque des appareils portables, des sauvegardes restaurables, un délai court avant le verrouillage de l'écran, le principe du moindre privilège et une procédure connue pour signaler un appareil perdu ou un message suspect. Le NIST recommande le chiffrement intégral du disque des ordinateurs portables et des tablettes. (tsapps.nist.gov) Pensez cybersécurité s'adresse directement aux petites entreprises et recommande un plan qui couvre les appareils personnels ; les conseils de sécurité physique de la GRC sont destinés au personnel du gouvernement du Canada et sont adaptés ici à titre de conseils pratiques, et non d'obligation légale pour le secteur privé. (www.getcybersafe.gc.ca) (www.getcybersafe.gc.ca) (www.nist.gov) (www.cyber.gc.ca) (rcmp.ca)

Les données quantitatives décrivent l'adoption des mesures de contrôle, et non la sécurité relative des lieux. Dans l'enquête de **2023** de Statistique Canada auprès des entreprises comptant **10 employés ou plus, 16 %** ont déclaré un incident de cybersécurité ; l'échantillon final comprenait **12 462 entreprises**, avec un **taux de réponse de 71 %**. Son champ exclut les microentreprises comptant moins de dix employés. Ni cette enquête ni les conseils concernant les lieux ne permettent d'établir une probabilité défendable qu'un café, un domicile ou un espace de coworking donné soit sécuritaire. Utilisez la matrice imprimable ci-dessous pour approuver une tâche précise et consigner la mesure de contrôle compensatoire ainsi que son responsable. (www150.statcan.gc.ca) (www150.statcan.gc.ca) (www150.statcan.gc.ca)

Introduction et contexte

Un travailleur autonome qui rédige une proposition publique dans un café, un employé d'une jeune entreprise qui examine des dossiers clients à domicile et un consultant qui participe à un appel privé chez un client s'exposent à des risques différents. Le même ordinateur portable peut être bien configuré dans chaque environnement, mais tout de même montrer des renseignements confidentiels à une personne à proximité, laisser des documents sur une imprimante ou se connecter à un point d'accès trompeur. Ce rapport compare le travail **à domicile, dans un café, en coworking et sur un site client** en tant qu'environnements de travail. Il indique si une tâche devrait y être effectuée et quelles conditions doivent être remplies au préalable. Le

Centre pour la cybersécurité considère l'accès physique et les réseaux Wi-Fi usurpés comme des enjeux du télétravail, et l'Australian Cyber Security Centre conseille d'éviter de consulter des renseignements sensibles dans les lieux publics. (www.cyber.gc.ca) (www.cyber.gov.au)

Dans ce guide, **public** désigne le contenu approuvé pour être vu par quiconque ; **interne** désigne le travail professionnel courant non public ; **confidentiel/client** désigne les données visées par un engagement envers un client ou dont l'exposition entraînerait un préjudice commercial important ; **réglementé/très sensible** désigne le travail dont les exigences contractuelles ou sectorielles justifient un examen par des personnes qualifiées en sécurité et en protection de la vie privée. Il s'agit de catégories décisionnelles rédactionnelles, et non de classifications légales. Une petite entreprise devrait consigner sa propre classification et toute restriction imposée par ses clients avant de choisir un espace de travail. Les mesures de base du Centre canadien pour la cybersécurité s'adressent aux organisations comptant moins de **500 employés**, mais ses conseils ne remplacent pas le jugement propre à une microentreprise sur les renseignements dont l'exposition aurait des conséquences plus graves. (www.cyber.gc.ca)

La liste de vérification distingue les **mesures de contrôle du travailleur**, les **mesures de contrôle de l'entreprise**, les **mesures de contrôle de la plateforme** et les **mesures de contrôle du fournisseur d'espace de travail**. Un établissement peut fournir une salle et une connexion ; il ne peut pas décider quel employé devrait accéder au dossier d'un client ni si un ordinateur portable personnel peut le conserver. Pensez cybersécurité conseille aux petites entreprises de définir les attentes concernant les activités effectuées sur les appareils personnels, tandis que le Centre pour la cybersécurité recommande de limiter l'accès aux besoins de chaque poste. (www.getcybersafe.gc.ca) (www.cyber.gc.ca) Lorsque des renseignements personnels sont en jeu, obtenez des conseils appropriés en protection de la vie privée ou en droit, adaptés au contexte de l'entreprise et du client ; les entreprises admissibles peuvent demander une consultation auprès du Commissariat à la protection de la vie privée du Canada. (www.priv.gc.ca)

Bureau à domicile

Possibilités

Un bureau à domicile donne généralement au travailleur le plus de contrôle sur l'orientation de l'écran, les portes, les appels et le rangement des documents papier. Il peut convenir au travail confidentiel si l'entreprise approuve l'appareil, si le réseau domestique est entretenu et si les autres membres du ménage ne peuvent ni voir ni entendre les renseignements. **Une pièce avec une porte** constitue une mesure de contrôle physique plus solide que le simple déplacement d'un ordinateur portable vers un coin plus tranquille. La GRC recommande d'aménager les espaces de télétravail de façon à limiter les regards de l'extérieur, et les conseils du gouvernement australien privilégient un lieu privé pour les réunions Web confidentielles. Les deux sources sont des recommandations gouvernementales adaptées à un milieu de travail privé. (rcmp.ca) (www.cyber.gov.au)

Pour un environnement de télétravail sécuritaire, choisissez le réseau domestique de façon réfléchie. Confirmez que le routeur est pris en charge et configuré selon les exigences de sécurité actuelles, que l'appareil de travail ne partage pas de fichiers avec les appareils du ménage et que les invités utilisent un réseau distinct si l'équipement le permet. Le Centre pour la cybersécurité explique que l'accès des invités ne

devrait pas exposer le réseau principal et conseille de séparer le trafic des invités du trafic habituel. (www.cyber.gc.ca) Un point d'accès personnel peut être préférable lorsque le réseau domestique est incertain, mais les mesures de contrôle de l'appareil, des comptes et de l'environnement physique demeurent à gérer.

Mise en pratique

La liste de vérification pratique à domicile est assez courte pour qu'une personne travaillant seule puisse la répéter : utiliser un compte approuvé, confirmer l'authentification multifacteur (MFA), permettre les mises à jour du système et des applications, vérifier l'état des sauvegardes, fermer la porte pour un appel avec un client et ranger les documents papier à la fin du travail. Pensez cybersécurité recommande l'authentification multifacteur lorsqu'elle est offerte ; le NIST recommande de tester les sauvegardes, plutôt que de simplement présumer qu'une sauvegarde existe. (www.getcybersafe.gc.ca) (www.nist.gov) (chamber.ca) Si un ordinateur partagé du ménage ne peut pas respecter les règles de l'entreprise concernant les appareils et la séparation des usages, utilisez un appareil géré ou effectuez la tâche ailleurs. Le Centre pour la cybersécurité privilégie les appareils appartenant à l'organisation, parce que celle-ci peut en contrôler les paramètres. (www.cyber.gc.ca)

Forces et limites

La force du domicile est le **contrôle de la pièce**. Ses limites sont l'entretien inégal du routeur, la présence d'autres personnes dans l'espace et la possibilité qu'un appareil perdu ou endommagé contienne aussi la seule copie locale. L'entreprise devrait conserver une sauvegarde de façon sécuritaire, idéalement avec une copie de récupération hors ligne des renseignements essentiels, et savoir comment joindre sa personne-ressource pour le soutien. (www.cyber.gc.ca) Un bureau à domicile est donc **approuvé sous conditions** pour le travail confidentiel/client lorsque ces mesures sont vérifiées. Le travail très sensible exige toujours une décision explicite du client ou d'un spécialiste, plutôt qu'une présomption générale concernant le travail à domicile.

Café et espace public

Possibilités

Un café est utile pour le travail dont le contenu peut être vu ou entendu sans risque. C'est un mauvais choix par défaut pour les dossiers clients, les renseignements financiers privés, les appels sensibles ou l'impression. L'Australian Cyber Security Centre conseille expressément de ne pas consulter de renseignements sensibles dans les lieux publics. Pensez cybersécurité met en garde contre une personne qui regarderait l'écran par-dessus l'épaule du travailleur. (www.cyber.gov.au) (www.getcybersafe.gc.ca) Un filtre de confidentialité et une place choisie avec soin réduisent l'observation occasionnelle, mais ne rendent pas privée une conversation confidentielle en direct.

Le Wi-Fi public mérite une réponse précise. Selon la FTC, le chiffrement des sites Web modernes fait en sorte que le Wi-Fi public est généralement sécuritaire pour la navigation Web courante, tandis que le Centre pour la cybersécurité recommande de l'éviter pour les activités professionnelles dans la mesure du possible. Ces affirmations sont compatibles : le chiffrement du transport atténue un risque réseau, mais une entreprise doit

tout de même évaluer les réseaux usurpés, les appareils exposés, la sécurité des applications et la sensibilité de la tâche. (consumer.ftc.gov) (www.cyber.gc.ca) Un point d'accès malveillant peut imiter le nom du réseau d'un café ; demandez donc au personnel le nom exact du réseau et désactivez la connexion automatique aux réseaux inconnus. (www.cyber.gc.ca) (www.getcybersafe.gc.ca)

Mise en pratique

Pour le travail portant sur des renseignements publics ou peu sensibles, utilisez un appareil pris en charge, l'authentification multifacteur, un écran verrouillé lorsque vous vous éloignez et un service chiffré connu. Si l'entreprise exige un accès par VPN, connectez-le avant d'utiliser les ressources de l'entreprise et confirmez qu'il demeure actif. Le Centre pour la cybersécurité indique que la sécurité du VPN dépend de sa configuration et de son utilisation constante, et le National Cyber Security Centre du Royaume-Uni souligne que seul le trafic acheminé par le VPN bénéficie de sa protection. (www.ncsc.gov.uk) En cas de doute sur un point d'accès, passez aux données cellulaires ou reportez la tâche.

Le travailleur doit garder l'appareil avec lui ou le ranger sous clé lorsqu'il ne peut pas le surveiller. Un câble antivol peut compliquer un vol, mais n'autorise pas à laisser des données clients sans surveillance. Les conseils de l'Université de la Colombie-Britannique suggèrent un câble antivol dans les espaces partagés ou publics, tandis que les conseils britanniques recommandent de garder sur soi ou de ranger sous clé un appareil qui ne peut être surveillé. (privacymatters.ubc.ca) (www.ncsc.gov.uk) Évitez les appels en mode mains libres, les documents imprimés sensibles et les notes visibles. Une séance de travail dans un espace public devrait avoir une fin claire : fermez l'application, rassemblez vos effets personnels et confirmez que l'appareil se reconnecte uniquement à un réseau voulu.

Forces et limites

La force d'un café est sa commodité pour les **tâches portant sur des renseignements publics ou peu sensibles**. Sa limite est l'absence de contrôle sur les personnes à proximité, l'administration du réseau et les conversations confidentielles. La règle est **non approuvé pour le travail confidentiel/client ou très sensible**, sauf si une exception précise a été examinée et si les mesures de contrôle compensatoires répondent réellement à chaque exposition. Un VPN ne peut pas empêcher l'hameçonnage ni l'observation par-dessus l'épaule. (www.getcybersafe.gc.ca) Pour la plupart des microentreprises, reporter une tâche sensible coûte moins cher et est plus simple que de tenter d'aménager une pièce privée dans un café ouvert.

Espace de coworking

Possibilités

Le coworking peut offrir des postes de travail, des salles de réunion et une personne-ressource pour le soutien, mais leur disponibilité varie selon le site et l'abonnement. La décision de sécurité devrait distinguer un **poste en aire ouverte** d'une **salle privée pouvant être réservée**, ainsi que les deux des mesures de contrôle propres à l'entreprise pour les comptes et les appareils. Les conseils de la GRC sur les espaces partagés recommandent des salles de réunion ou des salles calmes lorsqu'une conversation doit demeurer privée, des réseaux Wi-Fi distincts pour les visiteurs et les utilisateurs de l'espace partagé, ainsi qu'un point de contact

central pour les préoccupations de sécurité. Il faut préciser que ces conseils sont destinés à un contexte gouvernemental lorsqu'on adapte ces questions à un établissement commercial. (rcmp.ca) (rcmp.ca) (rcmp.ca)

Demandez au fournisseur si le trafic des invités et celui des membres sont séparés, si les appareils sur le même réseau sans fil peuvent communiquer entre eux, qui traite les problèmes de réseau et comment un travailleur peut signaler une préoccupation concernant la sécurité physique. Ce sont des **questions**, et non des affirmations selon lesquelles un établissement donné dispose de ces mesures de contrôle. Le Centre pour la cybersécurité recommande d'empêcher les appareils des invités d'interagir avec les appareils du réseau principal ; ce principe fait de la séparation une question pertinente à poser au fournisseur. Demandez si une salle privée est disponible pour un appel confidentiel et si l'impression nécessite un code de libération ou une récupération immédiate. La norme du secteur public de l'Ontario exige la récupération rapide des documents imprimés, une mesure de contrôle pratique utile à adapter sans la présenter comme une obligation pour les utilisateurs d'espaces de coworking privés. (www.ontario.ca)

Mise en pratique

Un membre devrait vérifier le nom du réseau voulu, appliquer les règles de l'entreprise concernant les appareils et l'authentification multifacteur (MFA), orienter l'écran et décider où ranger les documents papier à la fin de la séance de travail. C'est le travailleur, et non l'établissement, qui décide si un fichier peut être téléchargé sur un appareil personnel. Le Centre pour la cybersécurité recommande de définir les catégories de données auxquelles il est permis d'accéder ou qui peuvent être stockées sur du matériel utilisé dans le cadre d'une politique d'utilisation des appareils personnels (BYOD). (www.cyber.gc.ca) Avant une réunion sensible, utilisez une salle dont la porte et les conditions acoustiques ont réellement été vérifiées. Ne présumez pas qu'une cabine téléphonique, une salle partagée ou un système d'alarme contrôle le trafic réseau.

Forces et limites

Un espace de coworking peut être **approuvé sous conditions** pour le travail interne et, après une vérification précise, pour le travail confidentiel. Sa valeur supplémentaire tient à la possibilité d'avoir une salle privée et un endroit où poser des questions opérationnelles ; ni l'un ni l'autre ne rend l'établissement automatiquement sécuritaire. Par exemple, **2727 Coworking** annonce des postes flexibles / hot desks, des postes attitrés, des bureaux privés et une connexion Internet gigabit à Montréal, avec un poste flexible affiché à partir de **300 \$ par mois** en octobre 2026. Ses pages publiées n'établissent pas la segmentation du réseau, l'isolation des appareils ni une personne à joindre en cas d'incident touchant les données d'un client ; un utilisateur devrait interroger directement l'exploitant avant d'approuver du travail confidentiel. (2727coworking.com) (2727coworking.com) L'entreprise demeure responsable des autorisations d'accès, des sauvegardes et de l'intervention en cas d'incident. (www.getcybersafe.gc.ca)

Site client

Possibilités

Dans les locaux d'un client, celui-ci contrôle certaines conditions physiques et réseau, mais l'entreprise en visite demeure responsable de ses propres appareils, de ses comptes et du traitement de ses copies des renseignements. Un client peut fournir un poste de travail, un réseau pour invités, une imprimante ou une salle de réunion. Considérez chacun comme **non vérifié jusqu'à ce que le client explique l'utilisation permise**. Les mesures de base du Centre pour la cybersécurité indiquent que le Wi-Fi des visiteurs devrait être séparé des ressources internes, et les conseils de la GRC sur les espaces partagés préconisent une personne clairement désignée pour les signalements et un espace pour les conversations privées. (rcmp.ca) (rcmp.ca)

La question initiale est de savoir quelle partie fixe les règles qui régissent la tâche. Un consultant en visite devrait obtenir la méthode de connexion approuvée par le client et confirmer si le téléchargement local, les appareils personnels ou l'impression sont permis. Les conseils du Centre pour la cybersécurité sur l'utilisation des appareils personnels recommandent de préciser les données auxquelles il est permis d'accéder, ainsi que celles qui peuvent être créées ou stockées sur ces appareils. (www.cyber.gc.ca) Si le client fournit un poste informatique, ne présumez pas qu'il peut être utilisé pour les autres clients du visiteur. Utilisez des comptes distincts et uniquement les autorisations nécessaires au mandat, conformément aux conseils du NIST sur les comptes. (www.nist.gov)

Mise en pratique

Avant de commencer, confirmez la personne-ressource chez l'hôte, le réseau autorisé, la salle de réunion, la méthode de transfert de fichiers et la procédure d'élimination des documents papier. Gardez les appareils et les documents à vue pendant les déplacements ; les conseils de la GRC indiquent que les renseignements ou les biens sensibles ne devraient pas être laissés sans surveillance pendant le transport. (rcmp.ca) Pour les appels vidéo, partagez l'application nécessaire plutôt que l'ensemble du bureau lorsque c'est possible, comme le conseille l'Australian Cyber Security Centre. (www.cyber.gov.au) Au départ, récupérez les pages imprimées et les notes, fermez votre session sur un poste emprunté et consignez tout problème d'accès ou de document non résolu.

Forces et limites

Le site du client peut être le seul environnement approuvé pour certains travaux **réglementés ou très sensibles**, mais le fait d'être sur place n'autorise pas automatiquement toutes les méthodes de travail. Le client peut interdire un ordinateur portable personnel, exiger son propre environnement isolé ou restreindre ce qui peut quitter les locaux. L'entreprise devrait obtenir des instructions explicites pour le projet et un examen de sécurité par des personnes qualifiées lorsque la catégorie de renseignements comporte de lourdes conséquences. Un travailleur en visite ne devrait jamais déduire une autorisation légale de la présence d'un port réseau ou d'une imprimante. La décision pratique est **conditionnelle à l'autorisation du client** et à des mesures de contrôle documentées.

Comparaison des caractéristiques

Le *tableau 1* est une matrice imprimable qui associe les tâches aux lieux. « Sous conditions » signifie que la mesure de contrôle indiquée doit être vérifiée pour la tâche précise ; il ne s'agit pas d'un score de risque. Chaque ligne suppose un compte approuvé, l'authentification multifacteur (MFA), un appareil pris en charge, une sauvegarde et une personne à joindre pour les signalements. Les évaluations constituent la synthèse opérationnelle de ce rapport, fondée sur les conseils canadiens en cybersécurité, les conseils en sécurité physique et la distinction concernant le Wi-Fi public présentée ci-dessus. (www.getcybersafe.gc.ca) (rcmp.ca) (consumer.ftc.gov)

Lieu et tâche	Sensibilité du travail	Contrôle du réseau	Propriété de l'appareil	Écran et audio	Documents papier et impression	Stockage	Décision	Mesure de contrôle compensatoire	Responsable
Bureau à domicile	Public, interne ou confidentiel/client	Routeur domestique vérifié ; utilisation distincte pour les invités lorsque possible (www.cyber.gc.ca)	Appareil géré privilégié ; utilisation des appareils personnels (BYOD) selon une règle écrite (www.getcybersafe.gc.ca)	Porte, position de l'écran, appels privés (rcmp.ca)	Ranger les documents papier sous clé ; éviter les bacs des imprimantes partagées (mednet.med.ubc.ca)	Stockage infonuagique approuvé ou stockage local chiffré, avec sauvegarde	Approuvé sous condition pour le travail confidentiel ; le travail très sensible exige un examen	Connexion cellulaire de rechange, pièce privée, appareil géré	Entreprise et travailleur
Café ou espace public	Travail public ou interne peu sensible	Vérifier le nom du réseau ; utiliser une connexion cellulaire en cas de doute (www.getcybersafe.gc.ca)	Appareil géré privilégié	Présumer que les personnes à proximité peuvent voir et entendre (www.cyber.gov.au)	Aucune impression sensible ni note laissée à découvert	Éviter les copies locales confidentielles	Approuvé uniquement pour le travail peu sensible ; travail confidentiel normalement non approuvé	Reporter la tâche ou se déplacer dans une pièce privée	Entreprise et travailleur

Lieu et tâche	Sensibilité du travail	Contrôle du réseau	Propriété de l'appareil	Écran et audio	Documents papier et impression	Stockage	Décision	Mesure de contrôle compensatoire	Responsable
Poste en aire ouverte ou salle privée dans un espace de coworking en général	Interne ; confidentiel uniquement après vérifications	Poser des questions sur la séparation des membres, des invités et des appareils (rcmp.ca)	L'entreprise approuve l'appareil	Le poste en aire ouverte expose les écrans ; salle privée pour les appels (rcmp.ca)	Poser des questions sur la libération des travaux d'impression et l'élimination des documents (www.ontario.ca)	Stockage et sauvegarde gérés par l'entreprise	Approbation sous conditions , selon la tâche et la vérification de la salle et du réseau	Salle privée, connexion cellulaire, aucun téléchargement local	Entreprise, travailleur, fournisseur
2727 Coworking, Montréal	Mêmes règles de tâche que pour le coworking	Connexion Internet gigabit annoncée ; détails de sécurité du réseau à confirmer (2727coworking.com)	L'entreprise approuve l'appareil	Postes flexibles / hot desks et bureaux privés annoncés (2727coworking.com)	Confirmer sur place l'impression et l'élimination des documents	Stockage et sauvegarde gérés par l'entreprise	Approbation sous conditions , sans attestation de sécurité	Interroger l'exploitant sur la séparation et la personne à joindre en cas d'incident	Entreprise, travailleur, 2727 pour les faits concernant l'établissement
Site client	Tâches approuvées par le client uniquement	Utiliser la méthode autorisée du client	Respecter les règles du client et de l'employeur concernant les appareils	Confirmer les autorisations relatives aux salles et aux appels	Confirmer les règles du client concernant l'impression, la récupération et l'élimination des documents	Respecter les instructions du projet concernant l'emplacement des données	Sous réserve de l'autorisation du client	Instructions écrites pour la tâche et personnel-ressource chez l'hôte	Client, entreprise, travailleur

La matrice devrait être remplie pour une **tâche précise**, plutôt que servir de sceau accordé une fois pour toutes à un établissement. Un appel confidentiel peut être acceptable dans une salle privée en coworking, tandis que les mêmes renseignements ne devraient pas apparaître à un poste en aire ouverte. La mention « non approuvé » du tableau est un choix rédactionnel prudent par défaut pour les microentreprises, et non une affirmation selon laquelle les installations d'un fournisseur ont échoué à un test. Si le client impose des instructions plus strictes, celles-ci régissent le travail.

Le *tableau 2* répartit les responsabilités relatives aux mesures de contrôle. Les commodités physiques d'un établissement ne peuvent pas remplacer les décisions concernant les autorisations des comptes, les sauvegardes ou la classification des données. Pensez cybersécurité préconise un plan de cybersécurité d'entreprise, et le Centre pour la cybersécurité indique que les employés devraient savoir qui joindre lorsqu'un appareil est perdu. (www.getcybersafe.gc.ca)

Mesure de contrôle	Travailleur	Entreprise ou employeur	Plateforme ou service	Fournisseur d'espace de travail ou client hôte
Classification de la tâche et lieu permis	Respecter l'instruction	Définir la décision et les exceptions	Appliquer les autorisations d'accès aux données lorsqu'elles sont configurées	Préciser les restrictions du site et du client
Comptes et authentification multifacteur (MFA)	Utiliser son propre compte et répondre à la demande d'authentification	Accorder, examiner et retirer les accès (www.getcybersafe.gc.ca)	Fournir l'authentification multifacteur et les journaux	Gérer uniquement les comptes de l'établissement, s'il y en a
Appareil et mises à jour	Garder l'appareil verrouillé et signaler sa perte	Approuver la propriété, les mises à jour et le chiffrement	Offrir des mesures de contrôle des appareils lorsque le contrat le prévoit	Préciser les règles concernant l'équipement
Connexion	Vérifier le nom du réseau et l'état du VPN	Définir la politique de connexion	Protéger le trafic acheminé, selon la configuration (www.ncsc.gov.uk)	Expliquer la séparation entre invités et membres
Écrans, appels et documents papier	Orienter l'écran, utiliser une salle, récupérer les pages	Préciser le traitement permis	Offrir des mesures de contrôle du partage et du stockage	Fournir une salle et un processus d'impression, s'ils sont disponibles
Sauvegarde et intervention	Signaler rapidement	Tester la récupération et diriger l'intervention en cas d'incident (www.nist.gov)	Conserver ou restaurer les données selon le contrat	Fournir une personne-ressource pour le soutien de l'établissement (rcmp.ca)

L'entreprise est responsable de la décision finale d'approbation parce qu'elle comprend les données et les obligations envers les clients. La plateforme contrôle uniquement le service qu'elle fournit, et le fournisseur d'espace de travail contrôle uniquement ses installations et son réseau. Le propriétaire d'une entreprise individuelle peut remplir à la fois les colonnes du travailleur et de l'entreprise, mais devrait tout de même prendre chaque décision explicitement.

Le *tableau 3* est une fiche de questions à poser au fournisseur. Consignez la réponse, la date et le nom de la personne qui l'a donnée avant de vous fier à l'établissement pour du travail sensible. Les questions suivent les conseils du Centre pour la cybersécurité sur les réseaux pour invités et les recommandations de la GRC sur les espaces partagés, adaptés à un espace de travail commercial. (rcmp.ca) (rcmp.ca)

Questions pour l'espace de travail ou le client hôte	Ce qu'une réponse utile précise	En l'absence de réponse
Quel réseau est destiné aux membres, aux invités et au personnel ?	Noms exacts des réseaux et personnes autorisées à utiliser chacun	Utiliser un accès cellulaire approuvé ou reporter
Les appareils sur le réseau des membres ou des invités peuvent-ils communiquer entre eux ?	Politique d'isolation ou de séparation et personne-ressource pour le soutien	Ne pas déduire l'isolation de la présence d'un mot de passe Wi-Fi
Qui traite une préoccupation concernant la sécurité du réseau ou la sécurité physique ?	Fonction désignée et moyen de communication accessible	Obtenir une personne-ressource avant le travail sensible
Une salle privée est-elle disponible pour un appel avec un client ?	Accès à la salle et conditions de confidentialité audio	Déplacer ou reporter l'appel
Comment les travaux d'impression sont-ils libérés, récupérés et éliminés ?	Méthode de récupération et procédure d'élimination confidentielle	Ne pas imprimer de documents clients
Quelles sont les règles d'accès et d'utilisation de l'équipement ?	Heures, règles pour les visiteurs, appareils approuvés, rangement	N'apporter aucun équipement ni document papier sensible

Un **oui** n'a de sens que si la réponse concerne la méthode de travail réelle. « Nous avons le Wi-Fi » n'explique pas la séparation du réseau ; « nous avons des salles de réunion » ne confirme pas qu'une salle est disponible pour un appel donné. Consignez l'incertitude comme raison de choisir une tâche plus simple ou un autre lieu.

Performance et critères de référence

Les sources consultées ne contiennent aucun critère de référence public crédible et comparable qui attribue une probabilité de compromission à un bureau à domicile, à un café, à un poste en coworking ou à un site client. Les conseils disponibles recensent des mesures de contrôle et des expositions ; ce rapport utilise donc des **conditions de décision**, et non un score de lieu inventé. Un VPN peut protéger le trafic qui y transite, mais le Centre pour la cybersécurité indique qu'il ne protège pas contre le fait de cliquer sur des liens malveillants. (www.ncsc.gov.uk) Un bureau privé améliore les conditions audio et visuelles uniquement si le travailleur l'utilise réellement, tandis qu'un réseau correctement isolé répond à une autre voie d'exposition. (rcmp.ca)

Les critères de référence mesurables les plus proches concernent le **degré de préparation du programme**. Le Centre pour la cybersécurité accorde la priorité à quatre domaines de départ pour les petites et moyennes organisations : la planification des interventions en cas d'incident, l'application de correctifs, l'authentification forte et les sauvegardes avec chiffrement. (www.cyber.gc.ca) La fiche d'information fédérale de CyberSécurité Canada décrit un programme volontaire fondé sur **13 mesures de contrôle**. (ised-isde.canada.ca) Ni l'une ni l'autre de ces mesures ne certifie qu'un café ou un espace de coworking donné convient aux dossiers clients. Une petite équipe peut utiliser les catégories comme liste de vérification, puis tester ses propres capacités opérationnelles : peut-on verrouiller ou récupérer un appareil, restaurer une sauvegarde et désactiver rapidement un compte ? Le NIST recommande expressément de tester les sauvegardes. (www.nist.gov)

Cette distinction compte lorsqu'on compare la **sécurité à domicile et en coworking**. Un bureau à domicile peut offrir un meilleur contrôle sur les personnes à proximité, mais un soutien plus faible de la part du fournisseur ; un espace de coworking peut offrir une salle privée, tout en exigeant des vérifications supplémentaires sur le réseau partagé et l'impression. La réponse varie selon la tâche et les mesures de contrôle en place. La matrice du rapport consigne donc **l'approbation, la mesure de contrôle compensatoire et le responsable**, plutôt que de désigner un gagnant universel.

Analyse des données et éléments probants

Les données canadiennes disponibles décrivent les pratiques des entreprises en cybersécurité, et non la sécurité des lieux. L'Enquête canadienne sur la cybersécurité et le cybercrime de **2023** de Statistique Canada portait sur les entreprises comptant **10 employés ou plus** ; elle ne mesure donc pas directement les travailleurs autonomes ni les plus petites jeunes entreprises montréalaises. Son échantillon final comptait **12 462** entreprises, avec un taux de réponse de **71 %**. Environ **16 %** des entreprises interrogées ont déclaré avoir subi un incident de cybersécurité ; **26 %** ont déclaré avoir des politiques écrites de cybersécurité et **22 %** ont déclaré offrir une formation officielle aux employés qui ne travaillent pas en TI. Ces chiffres donnent un contexte utile pour comprendre pourquoi un court plan documenté compte, mais ils ne permettent pas de classer un café par rapport à un bureau à domicile. (www150.statcan.gc.ca) (www150.statcan.gc.ca) (www150.statcan.gc.ca)

Le sondage de **2022** de CIRA sur la cybersécurité a recueilli **500** réponses en ligne de responsables canadiens de la cybersécurité. **55 %** ont décrit leur organisation comme plus vulnérable parce que les employés travaillaient à distance. Il s'agit d'une perception des répondants, et non d'un taux d'incidents mesuré propre à un type de lieu. Le sondage de **2025** de CIRA, également fondé sur **500** responsables, indiquait que **98 %** des organisations des répondants offraient une formation en cybersécurité. La série de CIRA et l'enquête de Statistique Canada utilisent des populations et des formulations de questions différentes ; leurs chiffres sur la formation ne constituent donc ni une courbe de tendance ni une contradiction. (www.cira.ca) (www.cira.ca) (www.cira.ca)

Un sondage de **2024** de la Banque de développement du Canada indiquait que **11 %** des petites entreprises répondantes disposaient d'un plan officiel d'intervention en cas de cyberincident, tandis que les autres décrivaient un plan informel ou n'en avaient aucun. Le sondage fournit une indication générale, et non une probabilité pour une entreprise donnée. (www.bdc.ca) L'enquête de **2025 à 2026** du Commissariat à la protection de la vie privée du Canada auprès des entreprises indiquait que **65 %** utilisaient l'authentification multifacteur et **55 %**, le chiffrement des renseignements personnels des clients. Ces résultats d'enquête montrent une adoption déclarée inégale des mesures de contrôle, mais les populations et les méthodes diffèrent. Ils justifient de demander si une organisation précise a mis en place une mesure de contrôle plutôt que de présumer qu'elle l'a fait. (www.priv.gc.ca)

Pour une microentreprise donnée, la mesure quantitative la plus utile pour agir est **l'achèvement de la liste de vérification locale**, et non un pourcentage national emprunté. Consignez si chaque mesure de contrôle requise est présente, quand elle a été vérifiée pour la dernière fois et qui est responsable de la lacune. Si une tâche très sensible échoue à ne serait-ce qu'une seule condition requise, effectuez-la ailleurs ou demandez un examen par un spécialiste. Les conseils du Centre pour la cybersécurité sur les sauvegardes décrivent

plusieurs copies, dont une copie hors ligne, et le NIST recommande un test de restauration. Ce sont des vérifications concrètes qu'une petite entreprise peut effectuer sans inventer un score de risque.
(www.cyber.gc.ca) (www.nist.gov)

Implications et orientations futures

Une vérification de dix minutes avant le travail

Voici une liste de vérification **oui/non** pour une séance de travail. Un « non » signifie qu'il faut régler le point, réduire la sensibilité de la tâche ou changer de lieu. Dix minutes est un objectif pratique pour examiner une configuration déjà préparée, et non une affirmation selon laquelle un nouveau programme de sécurité peut être mis en place en dix minutes.

- **Tâche** : Les renseignements sont-ils classés comme publics, internes, confidentiels/client ou très sensibles, et ce lieu est-il permis ?
- **Règle du client** : A-t-on vérifié les instructions du contrat ou du projet concernant l'appareil, le réseau, la salle ou l'impression ?
- **Compte** : Le travailleur utilise-t-il un compte individuel approuvé avec l'authentification multifacteur (MFA) lorsqu'elle est offerte ? (www.cisa.gov)
- **Autorisations** : L'accès est-il limité aux fichiers nécessaires à cette tâche ?
- **Appareil** : L'appareil est-il approuvé, pris en charge, à jour, configuré pour le chiffrement intégral du disque et réglé pour se verrouiller lorsqu'il est sans surveillance ? (www.cyber.gc.ca) (tsapps.nist.gov)
- **Utilisation des appareils personnels (BYOD)** : Si l'appareil est personnel, les catégories de données permises et la méthode de suppression sont-elles consignées par écrit ? (www.cyber.gc.ca) (www.priv.gc.ca)
- **Réseau** : Le nom réel du réseau est-il vérifié, et une connexion cellulaire ou une autre solution de rechange approuvée est-elle disponible ? (www.getcybersafe.gc.ca)
- **VPN** : S'il est requis, est-il actif pour le trafic voulu, et ses limites sont-elles comprises ? (www.ncsc.gov.uk)
- **Écran** : Une personne à proximité peut-elle voir l'écran, le tableau blanc, les notes ou les notifications ? (www.getcybersafe.gc.ca)
- **Audio** : Une salle privée est-elle disponible pour un appel confidentiel ? (www.cyber.gov.au)
- **Documents papier** : Les documents imprimés seront-ils récupérés immédiatement et rangés ou éliminés correctement ? (www.ontario.ca)
- **Stockage** : L'emplacement approuvé pour les fichiers est-il disponible, avec une sauvegarde récente pouvant être restaurée ? (www.nist.gov)
- **Intervention** : Le travailleur sait-il qui joindre en cas de perte, d'hameçonnage ou de problème dans l'établissement ? (rcmp.ca)

Fiche d'intervention en cas d'appareil perdu ou d'hameçonnage soupçonné

Conservez cette fiche avec les instructions de travail, séparément de l'appareil. Elle attribue des **actions immédiates**, et non une procédure complète d'investigation numérique.

- **Appareil perdu** : Signalez immédiatement la perte à la personne-ressource de l'entreprise ; indiquez le dernier emplacement connu, l'identité de l'appareil et s'il contenait des fichiers clients locaux. Les conseils britanniques préconisent de joindre immédiatement le service de soutien. (www.ncsc.gov.uk)
- **Protéger les accès** : Demandez à l'administrateur des comptes de révoquer les sessions, de renouveler les renseignements d'authentification pertinents et d'envisager un effacement à distance préconfiguré ou un conteneur de données d'entreprise. Le Commissariat à la protection de la vie privée décrit un conteneur qu'une organisation peut effacer après la perte ou le vol d'un appareil personnel ; il ne promet pas que l'effacement fonctionnera lorsque l'appareil est hors ligne. (www.priv.gc.ca)
- **Demande suspecte** : N'utilisez pas les coordonnées de rappel du message. Vérifiez auprès d'un numéro connu ou par un moyen de communication déjà jugé fiable. (www.ftc.gov)
- **Clic ou saisie possible de renseignements d'authentification** : Joignez le responsable de l'entreprise ; changez les mots de passe compromis et isolez un appareil soupçonné de contenir un logiciel malveillant selon la procédure de l'entreprise. (www.ftc.gov)
- **Préserver le contexte** : Conservez le courriel ou le message texte suspect et les horodatages pertinents pour la personne chargée de l'intervention ; le Centre antifraude du Canada conseille de conserver des copies des messages et offre le signalement en ligne des fraudes ou des cybercrimes. (antifraudcentre-centreantifraude.ca) (antifraudcentre-centreantifraude.ca)

Une petite entreprise devrait faire un exercice pour vérifier qui reçoit l'appel et qui peut désactiver les comptes. Les conseils du Centre pour la cybersécurité sur le télétravail indiquent explicitement que les travailleurs devraient savoir qui joindre après un problème de sécurité ou la perte d'un appareil. Si des renseignements personnels peuvent être en jeu, obtenez des conseils appropriés en protection de la vie privée ou en droit, selon les faits et le territoire de compétence ; le Commissariat à la protection de la vie privée offre un service-conseil aux entreprises admissibles. (www.priv.gc.ca)

Foire aux questions (FAQ)

Est-il sécuritaire de travailler dans un café sur le Wi-Fi public ?

Pour la **navigation portant sur des renseignements publics ou peu sensibles**, souvent oui lorsque la connexion au site Web est chiffrée et que l'appareil est entretenu ; la FTC met expressément en garde contre le fait de considérer automatiquement tout Wi-Fi public comme dangereux. Pour le travail professionnel confidentiel, le Centre pour la cybersécurité conseille d'éviter le Wi-Fi public dans la mesure du possible, et l'espace ouvert ajoute une exposition visuelle et audio. Vérifiez le nom du point d'accès, utilisez une connexion approuvée par l'entreprise et déplacez les appels et les dossiers sensibles vers un environnement privé. (consumer.ftc.gov) (www.getcybersafe.gc.ca) (www.cyber.gov.au)

Que devrait inclure une microentreprise canadienne dans sa liste de vérification de cybersécurité pour le télétravail ?

Au minimum : la classification de la tâche ; un compte approuvé et l'authentification multifacteur ; un appareil pris en charge et à jour ; des règles claires pour l'utilisation des appareils personnels ; un réseau connu ; la confidentialité de l'écran et des appels ; des documents papier contrôlés ; une sauvegarde restaurable ; des

autorisations limitées ; et une personne à joindre pour les signalements. Cette séquence combine les conseils de planification de Pensez cybersécurité pour les petites entreprises et les mesures techniques et d'intervention du Centre pour la cybersécurité. (www.getcybersafe.gc.ca) (www.getcybersafe.gc.ca)

Un espace de coworking est-il plus sécuritaire qu'un bureau à domicile ?

Aucun des deux environnements ne l'emporte automatiquement. Le travailleur à domicile peut contrôler la pièce et le réseau domestique, tandis qu'un fournisseur de coworking peut offrir une salle privée et une personne-ressource pour le soutien. Posez des questions sur la séparation réelle du réseau et les conditions de la salle, puis approuvez la **tâche précise** dans la matrice. Les conseils de la GRC sur les espaces partagés font de la séparation du réseau et des salles permettant la confidentialité des questions pertinentes ; il s'agit de conseils gouvernementaux adaptés à cette décision commerciale. (rcmp.ca) (rcmp.ca) (rcmp.ca)

Un VPN peut-il rendre le travail pour un client sécuritaire partout ?

Non. Un VPN couvre uniquement le trafic qui y transite et ne bloque pas les liens malveillants, n'empêche pas une personne de regarder un écran ni une conversation d'être entendue. Utilisez-le lorsque l'entreprise l'exige, avec l'authentification multifacteur, la sécurité des appareils et une salle appropriée. (www.ncsc.gov.uk) (www.cyber.gov.au)

Conclusion

L'unité d'approbation utile est **une tâche dans un lieu précis avec des mesures de contrôle vérifiées**. Le domicile peut convenir au travail confidentiel lorsque la pièce, le réseau, l'appareil, la sauvegarde et la procédure d'intervention sont contrôlés. Un café convient généralement au travail portant sur des renseignements publics ou peu sensibles. Le coworking peut convenir à des tâches plus sensibles après l'obtention de réponses utilisables aux questions sur la séparation du réseau, les salles privées, le traitement des documents papier et le soutien. Un site client exige l'autorisation propre au client et ses règles de travail.

Pour une petite entreprise canadienne, le point de départ est un appareil approuvé, un compte individuel, l'authentification multifacteur (MFA), les mises à jour, le principe du moindre privilège, une sauvegarde pouvant être restaurée et une personne désignée à joindre en cas d'incident. Le travailleur vérifie ensuite l'identité du réseau et l'exposition physique avant chaque séance de travail. Un établissement fournit une partie de l'environnement ; l'entreprise fournit la décision concernant les renseignements et les accès. Utilisez la matrice et la fiche oui/non comme documents opérationnels évolutifs, et soumettez les questions sur les renseignements très sensibles ou personnels à un examen par des personnes qualifiées. L'objectif est un processus d'approbation reproductible qu'un travailleur autonome ou une petite équipe peut réellement appliquer.

Liens vers les sources

Liens cités dans cet article, dans leur ordre de première apparition. Les adresses complètes sont fournies pour les lecteurs qui utilisent le texte extrait.

1. <https://www.cyber.gc.ca/en/guidance/telework-security-issues-itsap10016>

2. <https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know>
3. <https://www.cyber.gc.ca/en/guidance/protecting-your-organization-while-using-wi-fi-itsap80009>
4. <https://www.cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations>
5. <https://www.ncsc.gov.uk/collection/device-security-guidance/infrastructure/virtual-private-networks>
6. <https://www.cyber.gc.ca/en/guidance/virtual-private-networks-itsap80101>
7. <https://www.getcybersafe.gc.ca/en/secure-your-connections/public-wi-fi>
8. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=957322
9. <https://www.getcybersafe.gc.ca/en/blogs/staying-cyber-safe-when-your-employees-work-remotely>
10. <https://www.getcybersafe.gc.ca/en/resources/get-cyber-safe-guide-small-businesses>
11. <https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics>
12. <https://rcmp.ca/en/lead-security-agency-physical-security/guidance-and-publications/gcpsg-008-2022-physical-security-considerations-remote-and-telework-environments>
13. <https://www150.statcan.gc.ca/n1/daily-quotidien/241021/dq241021a-eng.htm>
14. <https://www.cyber.gov.au/protect-yourself/staying-secure-online/security-tips-remote-working>
15. <https://www.priv.gc.ca/en/about-the-opc/what-we-do/advisory-services-businesses/>
16. <https://www.cyber.gov.au/business-government/protecting-devices-systems/remote-working-secure-mobility/remote-working/web-conferencing-security>
17. <https://www.cyber.gc.ca/en/guidance/guest-wi-fi-itsap80023?wbdisable=true>
18. <https://chamber.ca/canadian-small-business-cyber-security-survival-guide/>
19. <https://www.cyber.gc.ca/en/guidance/security-considerations-mobile-device-deployments-itsap70002>
20. <https://www.cyber.gc.ca/en/guidance/tips-backing-your-information-itsap40002>
21. <https://privacymatters.ubc.ca/news/your-laptops-quiet-vulnerabilities>
22. <https://www.ncsc.gov.uk/guidance/end-user-devices-advice-end-users>
23. <https://rcmp.ca/en/lead-security-agency-physical-security/guidance-and-publications/gcpsg-023-2025-physical-security-considerations-shared-space>
24. https://www.ontario.ca/page/go-its-250-general-security-requirements?redirect_id=document%2Fgo-its-250-general-security-requirements&redirect_year=2021
25. <https://www.cyber.gc.ca/en/guidance/end-user-device-security-bring-your-own-device-byod-deployment-models-itsm70003>
26. <https://2727coworking.com/>
27. <https://2727coworking.com/virtual-tour/>
28. <https://www.nist.gov/cyberframework/csf-11-quick-start-guide>
29. <https://mednet.med.ubc.ca/resources/facilities/hybrid-work-sharing-space/additional-resources-frequently-asked-questions-faqs/>
30. <https://www.cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035?UTMmessage=2024-05-30+-+Bulletin+CPA+-+Contacts>
31. <https://ised-isde.canada.ca/site/cybersecure-canada/en/cybersecure-canada-information-sheet>
32. <https://www.cira.ca/en/resources/documents/cybersecurity/2022-cira-cybersecurity-survey/>
33. <https://www.cira.ca/en/resources/documents/cybersecurity/2025-cybersecurity-survey/>

34. <https://www.bdc.ca/en/articles-tools/blog/cyberattacks-small-businesses-remain-denial>
35. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2026/por_bus_2025-26/?wbdisable=true
36. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/require-multifactor-authentication>
37. https://www.priv.gc.ca/en/privacy-topics/employers-and-employees/mobile-devices-and-online-services-at-work/gd_byod_201508/?wbdisable=true
38. <https://www.ftc.gov/business-guidance/small-businesses/cybersecurity>
39. <https://antifraudcentre-centreantifraude.ca/scams-fraudes/victim-victime-eng.htm?t=tools&wbdisable=true>

L'ÉDITEUR

À propos de 2727 Coworking

2727 Coworking is a Montreal workspace and business-address provider. We serve people who need a place to focus, meet, run a small business or establish a professional mailing presence. Our website offers English and French information about workspace options and services, alongside educational resources for operating a business in Canada.

A workspace that fits the day

Our workspace options include private offices, day passes and desks, and a conference room. These formats help individuals and teams compare a dedicated office with more flexible ways to work or hold a meeting. Prospective members can explore the virtual tour, review current pricing and book a visit before choosing a workspace.

Business addresses and mail

2727 Coworking provides business-address and virtual-mailbox services. Our resources explain the documents and practical questions involved, including guidance for people outside Canada. Service eligibility, included features, availability and access arrangements should be confirmed on the applicable service page or with our team.

Resources for Canadian small businesses

We publish guides, research and planning tools about workspace decisions, business addresses and starting a business in Canada. Our incorporation research includes information for people inside Canada and abroad, with jurisdiction-specific material to help readers identify the next questions to investigate. These educational resources complement our workspace and address services; they are not individualized legal, tax or immigration advice.

Visit or contact 2727 Coworking

Explore [private offices](#), [day passes and desks](#), [the conference room](#), [business addresses](#) and [virtual mailboxes](#). [Book a visit](#) or [contact the team](#) to discuss your needs.

A business address alone does not establish tax residence, immigration status, banking approval or eligibility for a government program.

Site Web : <https://2727coworking.com>

Cet article est de nature informative. Validez toute décision médicale, juridique, financière, réglementaire ou technique importante auprès de professionnels compétents et des sources primaires citées. Les services de l'entreprise sont décrits séparément des constats de recherche de l'article.