CONFORMITÉ

LIGNE DIRECTRICE I SÉCURITÉ DES ESPACES DE TRAVAIL EXTÉRIEURS

Ce document s'adresse à :
Tous courtiers individuels ou incorporés autorisés avec le Centre Financier Optimal Inc.

JANVIER 2018

425 NOTRE-DAME ST, DIEPPE NB E1A 9G4 | COMPLIANCE@OPTIMALCENTRE.CA | OPTIMALCENTRE.CA

INTRODUCTION

Objectif

La présente ligne directrice aide à assurer que des pratiques raisonnables en matière de sécurité sont appliquées dans les emplacements et espaces de travail situés à l'extérieur des immeubles gérés par le Centre Financier Optimal Inc. Pour fin de politique, nous allons se référer au terme Optimal pour identifier le Centre Financier Optimal Inc.

Vous êtes tenu de vous conformer en tous points aux exigences règlementaires et législatives, et ce, lorsque vous travaillez hors des locaux de la Optimal, dans votre propre bureau professionnel. En un mot, la mise en place d'un tel lieu de travail doit être faite de manière à minimiser le risque autant que possible.

La présente ligne directrice donne un aperçu des mesures de sécurité minimales que vous devriez mettre en œuvre dans les espaces de travail.

LIGNES DIRECTRICES GÉNÉRALES

1. Suivre toutes les pratiques et procédures commerciales applicables.

Vous devez vous conformer à toutes les politiques, normes, pratiques commerciales et procédures applicables, notamment les suivantes :

- Les Normes concernant l'usage acceptable des outils technologiques
- Les Normes de classification des données
- Le Code de conduite à l'intention des conseillers de Optimal
- Le document Protection des données sur le client : Sécuriser le matériel et les médias personnels

2. Sécuriser l'espace de travail

Suivez les directives suivantes pour sécuriser l'emplacement où seront situés l'espace de travail et l'équipement qui y sera utilisé :

- Assurez la confidentialité de tous les dossiers papier; veillez notamment à les garder sous clé lorsqu'ils ne sont pas utilisés.
- Si des documents doivent être détruits à l'emplacement extérieur, servez vous d'une déchiqueteuse avec coupe en travers.
- Si vous partagez un espace de travail avec un tiers, veillez à ce que les autres personnes n'aient accès ni aux dossiers des clients ni aux ordinateurs, par exemple.

- Si vous partagez du personnel administratif avec un tiers, assurez-vous que les dossiers et fichiers papier et électroniques des différents conseillers sont conservés séparément. De plus, le personnel administratif devrait signer des ententes de confidentialité.
- Prenez des précautions raisonnables pour protéger l'équipement et les fournitures contre le vol et un accès inapproprié.

Voici des exemples de mesures de sécurité pouvant être adoptées :

- Protection du matériel (p. ex. les ordinateurs portables) au moyen de câbles de verrouillage ou d'autres moyens adéquats
- Alarme antieffraction ou système de sécurité
- Local pour bureau distinct (fermant à clé) pour la conduite des affaires, y compris un emplacement pour les imprimantes, télécopieurs, numériseurs, photocopieuses, etc.
- Dispositifs de stockage résistants au feu
- Espace de rangement entièrement distinct
- Plaques multiprises (avec para-sustenteurs) et, possiblement, système d'alimentation sans coupure (ASC)
- Possibilité d'ententes de confidentialité pour les tiers fournisseurs de service, par exemple le soutien technologique ou l'entretien ménager

3. Sécuriser les communications

Veillez à ce que toutes les voies de communication entre votre emplacement et les autres bureaux soient sécurisées :

- N'utilisez que les moyens autorisés pour brancher des ordinateurs à votre réseau, y compris les routeurs recommandés, au besoin.
- Lorsque vous avez recours à une connexion sans fil, prenez les mesures appropriées pour éviter que votre ordinateur fasse l'objet d'un usage malhonnête.
- Assurez-vous que les clients comprennent que le courriel ne constitue pas un moyen sûr de transmettre des renseignements personnels, à moins que des mesures adéquates ne soient prises (c.-à-d. utiliser des mots de passe).
- Envisagez de recourir à des services de téléphonie et de messagerie vocale distincts afin de garantir le respect de la confidentialité et de la vie privée, et utilisez des scénarios professionnels appropriés.
- Assurez-vous que toutes les caractéristiques de sécurité des télécopieurs sont activées et que les appareils sont conservés en lieu sûr.
- Faites seulement appel à un service de messagerie reconnu et réputé dont la responsabilité, le suivi et les niveaux de service sont préétablis.
- Assurez-vous que tous les colis que vous envoyez et recevez nécessitent une signature et ne sont pas laissés à la porte.
- Lorsque vous déplacez des renseignements personnels ou confidentiels sur les clients d'un lieu à un autre, prenez les mesures nécessaires pour le faire en toute sécurité.

Par exemple :

- N'apportez que les renseignements dont vous avez besoin; prenez note des renseignements et des dossiers que vous apportez pour vous protéger en cas de perte ou de vol; rangez hors de la vue les dossiers papier et les appareils électroniques comprenant de l'information (dans le coffre des véhicules); et transportez les ordinateurs portables dans des sacs discrets.
- Éteignez complètement votre portable lorsque vous ne l'utilisez pas ou pendant son transport, afin que le chiffrement du disque dur soit activé.

4. Prévoir des sauvegardes périodiques

Créez et mettez en œuvre des processus et des procédures de secours informatique qui répondront à des besoins de base de reprise de l'exploitation ou à des exigences en matière de planification de la continuité des affaires.

Appliquez les critères suivants, selon vos exigences en ce qui a trait aux sauvegardes informatiques :

- Fréquence (quotidiennement, hebdomadairement, etc.)
- Rotation (au retour au bureau de la Compagnie, d'un autre bureau extérieur, etc.)
- Média (cédéroms, clés USB, bandes de sauvegarde)
- Entreposage (p. ex. coffre-fort maison ou classeur verrouillable, résistant au feu idéalement)
- Journalisation (enregistrement des sauvegardes)
- Tests (pour vous assurer que les sauvegardes sont utilisables)
- Destruction des sauvegardes conformément aux calendriers de conservation qui s'appliquent

5. Utiliser l'équipement et l'information correctement

Utilisez l'équipement conformément aux Normes concernant l'usage acceptable des outils technologiques et aux Normes de classification et de traitement des données.

Vous devez notamment respecter les règles ci-dessous :

- Vous ne devez ni désactiver ni modifier les dispositifs de sécurité de tout
- équipement qui vous est fourni ou qui est configuré à votre intention.
- Les renseignements confidentiels doivent toujours être stockés en lieu sûr, de préférence sur le lecteur réseau d'un serveur.
- Ne conservez que l'information nécessaire dans les assistants numériques personnels, téléphones cellulaires et dispositifs de stockage externes.
- Ne permettez pas aux membres de la famille, aux amis ou à quiconque n'y
- étant pas autorisé d'utiliser l'équipement ou les renseignements sur les clients qui vous ont été confiés ou d'y accéder.

- Assurez-vous qu'un écran de veille protégé par mot de passe s'affiche chaque fois que vous laissez un ordinateur sans surveillance.

Lorsque vous achetez ou louez un photocopieur ou d'autres appareils d'impression multifonctions, envisagez de prendre les mesures suivantes :

- Songez à faire affaire avec un fournisseur offrant des produits assortis de caractéristiques avancées de protection des données.
- La mémoire interne de l'appareil devrait s'effacer quand on l'éteint.
- Si l'appareil comporte un disque dur, celui-ci devrait être crypté et les données qu'il renferme devraient être supprimées de manière sécurisée.
- Si elles ne sont pas requises, les fonctions de numérisation ou d'envoi de télécopie sur le disque dur et d'impression réseau devraient être désactivées.
- Songez à faire enlever et détruire le disque dur avant de retourner l'appareil au fournisseur, à la fin du contrat de location.

6. Signaler immédiatement toute brèche de sécurité présumée ou constatée

Signalez tout incident relatif à la sécurité immédiatement.

Voici quelques exemples de brèches de sécurité :

- Vol de matériel informatique, y compris les assistants numériques personnels et les téléphones intelligents, contenant des données sur les clients.

Il faut aviser sans délai la Vérification de la conformité générale d'Optimal de tout incident ou brèche de sécurité.

Il faut également informer la Vérification de la conformité générale de toute divulgation possible de renseignements sur les clients.

Pour ce faire, veuillez communiquer avec :
Le chef de la vérification de la conformité chez le Centre Financier Optimal Inc.