TÉLÉTRAVAIL

Consignes pour l'utilisation des équipements de la Ville

Seuls les membres du personnel ayant obtenu l'autorisation de leur gestionnaire auront la possibilité d'utiliser un ordinateur fourni par l'employeur pour effectuer du télétravail.

Consignes générales

- L'usage des connexions VPN *(*FortiClient ou Pulse Secure*)* vous permettra d'accéder aux ressources internes suivantes à partir d'un poste de travail **fourni par la Ville :**
    - Les documents de votre direction qui sont enregistrés sur les différents lecteurs réseau (N:\, P:\, etc.).
    - Les applications corporatives comme : *Espace Client*, *Dyna*, *Guide TI*, Juris, *LevisVIP 7G*, *U4*, etc.

- Les employés désirant travailler sur des fichiers (feuille de temps, frais de déplacement, etc.), peuvent le faire depuis leur espace personnel *OneDrive* fourni par la Ville. Espace personnel

- L'utilisation de l'outil collaboratif *Teams* est permise pour le travail en équipe. Cet outil vous permet d'effectuer du clavardage, d'organiser des réunions virtuelles, d'effectuer du partage d'écran et de collaborer à plusieurs sur les documents des équipes Teams existantes. Espace collaboratif

Usage interdit

- Concernant les dossiers et les fichiers contenus dans les lecteurs réseau de la Ville (N:\, P:\, etc.) :
  Il est strictement défendu de déplacer ou de copier ces données sur des périphériques de stockage tel que des clés USB, disques durs externes ou sur des emplacements de stockage infonuagique qui ne sont pas fournis par la Ville (*DropBox*, *Google Drive*, etc.).

  Il est toutefois permis de copier temporairement un document vers l'espace personnel *OneDrive* et l'espace collaboratif *Teams* fournis par l'employeur. À la suite de l'utilisation de ce document, vous devrez le sauvegarder à nouveau dans son répertoire d'origine (N:\, P:\, etc.).

  Les objectifs de ces restrictions sont d'assurer la confidentialité des données de la Ville avec la sécurité déjà en place, de limiter les problèmes de liaisons croisées entre les fichiers et de minimiser la confusion lorsque la situation reviendra à la normale.

  En cas de doute, référez-vous à votre gestionnaire. Il communiquera au besoin avec l'équipe de la Direction des technologies de l'information pour proposer des solutions répondants aux cas particuliers.

Dossier informatisé du personnel

- Il n'est pas nécessaire de se connecter par VPN pour accéder au dossier informatisé du personnel. Les employés sont invités à utilise le lien suivant : https://portailemployes.ville.levis.qc.ca/

Rappel de quelques conseils en matière de sécurité

1. N'ouvrez aucun courriel douteux
Vous recevez peut-être des courriels provenant d'expéditeurs, connus ou inconnus, qui peuvent sembler suspects lorsqu'ils sont affichés dans le volet de prévisualisation. Quand cette situation se présente, n'ouvrez pas le courriel, qu'il soit accompagné ou non d'une pièce jointe.

Les courriels frauduleux peuvent contenir des pièces jointes ou des hyperliens malicieux. En cas de doutes, si vous connaissez l'expéditeur, communiquez avec lui par téléphone pour vous assurer de la légitimité du courriel. Si vous décidez de répondre à des courriels provenant de personnes ou d'organismes qui vous sont inconnus, évitez de transmettre de l'information personnelle.

2. Soyez prudents avec vos mots de passe
Ne partagez pas et ne laissez pas traîner vos mots de passe sur un papier. Vous êtes imputable de ce qui est fait avec votre compte. Chaque employé est censé avoir ses propres identifiants.

N'utilisez jamais un même mot de passe dans différents systèmes, car si une personne malintentionnée venait à découvrir celui-ci, elle aurait accès sans difficulté à toutes vos données. Privilégiez un mot de passe unique pour chaque besoin.

3. Verrouillez toujours votre poste de travail lorsque vous vous absentez
Même si vous vous absentez pour une courte durée, une personne malintentionnée pourrait profiter de ce moment pour poser des actions ou pour accéder à des informations auxquelles elle n'a habituellement pas accès.

Comme vous êtes imputable de ce qui est fait avec votre identifiant, verrouillez votre session dès que l'appareil n'est plus sous votre surveillance.

4. Signalez tout incident suspect
Si vous êtes témoin d'une situation qui vous semble anormale ou d'un usage inapproprié quant à l'utilisation des outils informatiques, soyez responsable et informez votre supérieur immédiatement.

Cette liste de conseils n'est pas exhaustive et l'informatique est en constante évolution. Si vous avez des doutes sur une situation, ne prenez aucun risque.

La Direction des technologies de l'information