Guide et exigences technologiques pour le télétravail à l'UMCS

Université de Moncton,
campus de Shippagan

Dernière mise à jour :
18 août 2023

1. INTRODUCTION

Le présent guide a pour objectif d'orienter le personnel de l'Université de Moncton, Campus de Shippagan et de faire connaître les exigences technologiques en matière de télétravail. Il ne remplace pas les politiques officielles de l'Université de Moncton (UMoncton) ou la politique d'utilisation du réseau universitaire. Ce guide définir un standard pour minimiser les risques et dommages potentiels associés à la sécurité informatique, à la perte ou l'accès non autorisé à des données confidentielles ou encore pour minimiser les risques de dommages aux systèmes informatiques de l'Université de Moncton.

2. PRÉALABLES AU TÉLÉTRAVAIL

2.1 Gestion des données

2.1.1 Données sur les espaces réseau

À moins d'exception, l'utilisation des espaces réseau de l'UMCS pour l'entreposage de données n'est pas permise pour le télétravail. Afin d'être éligible au télétravail, le membre du personnel devra entreposer ses données sur des services infonuagiques préapprouvés par la Direction générale des technologies (DGT) et le service des technologies de l'UMCS. Les services infonuagiques Microsoft 365 du domaine UdeM sont les services infonuagiques approuvés pour l'entreposage des données des utilisateurs et services.

Le service des technologies est disponible pour aider les départements à migrer leurs données aux services infonuagiques.

L'utilisation du service infonuagique n'ayant pas été préapprouvé est strictement interdite.

Le transfert de données institutionnelles par périphériques (clé USB, disque dur externe) n'est pas permis.

2.2 Formation en cybersécurité

Afin d'être éligible au programme de télétravail, le membre du personnel doit avoir complété les formations de base en cybersécurité, ainsi que le module portant spécifiquement sur le télétravail.

2.3 Service de téléphonie

Les membres du personnel sont encouragés à utiliser la plateforme Teams pour les communications avec leurs collègues de travail.

2.4 Membres du personnel qui utilisent les services Socrate, Perceptive et/ou Argos

Les membres du personnel qui utilisent les services Socrate, Perceptive et/ou Argos ont besoin d'une connexion à un réseau privé virtuel (RPV) afin d'accéder à ces applications. Ils doivent contacter le service des technologies pour faire installer le RPV sur leur ordinateur.

2.4.1 Réseau privé virtuel (RPV)

L'employé avec privilèges de RPV est responsable de s'assurer qu'aucun utilisateur non autorisé n'accède au réseau interne de l'Université de Moncton via les privilèges qui lui sont accordés;

L'utilisation de RPV est contrôlée à l'aide d'un mot de passe pour l'authentification de l'usager;

Tout ordinateur se branchant par RPV aux réseaux de l'Université de Moncton doit obligatoirement posséder un antivirus à jour, un logiciel anti-espion, un pare-feu (firewall) personnel actif et les plus récentes mises à jour de sécurité du système d'exploitation utilisé.

La durée limite d'une connexion au serveur RPV est de huit heures consécutives ;

Seuls les clients RPV spécifiés par les services de technologies de l'information et de communications des constituantes peuvent être utilisés;

Les utilisateurs prévoyant utiliser un ordinateur n'appartenant pas à l'Université pour accéder au RPV devront obligatoirement apporter leur ordinateur au service de TI de leur campus pour que le personnel technique s'assure que l'ordinateur possède les composantes de sécurité énumérées ci-haut. Les utilisateurs doivent comprendre que leurs appareils deviennent une extension des réseaux informatiques de l'Université de Moncton et qu'en soi, sont sujets aux mêmes règlements et politiques que ceux en vigueur pour les équipements de l'Université de Moncton.

3. ÉQUIPEMENTS TECHNOLOGIQUES

3.1 Équipements et services fournis par l'Université

3.1.1 Ordinateur

Le membre du personnel doit utiliser un ordinateur étant la propriété de l'Université.

Le membre du personnel doit s'assurer avec le service des technologies que le disque dur utilisé pour le télétravail est crypté.

L'ordinateur de l'UMoncton utilisé à la maison devra être verrouillé ou éteint lorsqu'il n'est pas en utilisation par le membre du personnel. L'utilisation de l'ordinateur de l'UMoncton est strictement réservée au membre du personnel pour lequel il a été désigné.

À la fin de la journée de travail, l'ordinateur devra être éteint.

3.1.2 Service TI à distance

Le service des technologies supportera à distance la plupart de ses services habituels, et fera les efforts jugés raisonnables pour accommoder la clientèle qui est en télétravail. Cependant, il est possible qu'il soit impossible ou inefficace de régler certains problèmes à distance alors, dans ce cas, le membre du personnel devra se rendre à son campus avec son ordinateur.

3.2 Équipements et services étant la responsabilité du membre du personnel

3.2.1 Lieu de travail

Le lieu de travail (typiquement à la résidence) doit être approuvé par l'UMoncton.

À noter qu'il est interdit d'avoir à proximité de son lieu de travail un assistant personnel ou une enceinte intelligents tel que Amazon Alexa, Google Home, Apple HomePod ou autres puisque ces appareils sont en mode d'écoute continue et peuvent mettre à risque les informations personnelles et confidentielles de l'institution.

3.2.2 Connexion Internet

Le membre du personnel est responsable de se procurer un service Internet haute vitesse avec un fournisseur externe.

Lors du télétravail, le membre du personnel peut utiliser une connexion Internet branchée avec câble Ethernet ou WiFi. Les branchements avec fils Ethernet sont généralement plus fiables, mais, souvent, il n'est pas convivial d'apporter une connexion filaire à l'espace de travail. La plupart des ordinateurs de bureau gérés par l'UMoncton, contrairement aux ordinateurs portables, n'ont pas accès au WiFi. Dans le cas où le membre du personnel veut utiliser un ordinateur de bureau avec WiFi, un adaptateur USB-Wifi sera nécessaire. Ceux-ci sont en vente chez des détaillants, les sites de commerce en ligne, etc.

Dans le cas où le membre du personnel n'est pas capable de régler des problèmes de connexion Internet (pare-feu local, etc.), la direction pourrait exiger que l'employé retourne travailler au bureau.

Les services de connexion WiFi doivent être protégés par un mot de passe.

Les réseaux WiFi multi résidence ne sont pas permis. Le service WiFi doit être unique à la résidence du membre du personnel.

3.2.3 Imprimante

Que ce soit au bureau ou en télétravail, les membres du personnel sont encouragés à utiliser

des solutions numériques de documentation et d'éviter les impressions papier. Dans le cas où cette politique ne peut pas s'appliquer à votre type de travail, et que vous pensez avoir besoin d'une imprimante, vous êtes invité à discuter de cette situation avec votre supérieur. Tous documents en format papier associé au travail doivent être entreposés de façon à en assurer la confidentialité.

3.2.4 Clavier, souris, casque d'écoute et autres périphériques

L'UMoncton fournit les périphériques nécessaires pour le travail au bureau. Lorsque le membre du personnel choisit de ne pas transporter ceux-ci à la maison et de retour au bureau, il est responsable de se procurer les équipements nécessaires à ses propres frais.

3.2.5 Branchement du poste de travail à la maison

Les branchements de l'ordinateur et des périphériques à la maison sont la responsabilité du membre du personnel.