ANNEXE 1

UNIVERSITÉ
DU QUÉBEC
EN OUTAOUAIS

GUIDE D'UTILISATION DES ACTIFS INFORMATIONNELS EN SITUATION DE TÉLÉTRAVAIL

Mise à jour le 13 novembre 2025

TABLE DES MATIÈRES

1 PRÉAMBULE

En mode télétravail, les membres du personnel utilisent Internet et les technologies de l'information pour accomplir leurs tâches professionnelles, il devient donc essentiel d'adopter des comportements sécuritaires afin de minimiser les risques en matière de sécurité de l'information et de sécurité informatique.

2 OBJECTIF

Le présent guide vise à recommander des mesures sécuritaires à adopter pour les utilisateurs qui effectuent du télétravail, et ce, afin de protéger les actifs informationnels de l'UQO.

2.1. Cadre externe à l'UQO

- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., c. A-2.1) ;
- *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (L.R.Q., c. G-1.03);
- *Loi sur les archives* (L.R.Q., c. A-21.1).

2.2. Cadre interne à l'UQO

- *Politique concernant l'accès et la protection des renseignements personnels;*
- *Politique concernant la gestion des documents, des archives et du patrimoine documentaire*;
- *Politique relative à la gestion et à la sécurité des actifs informationnels*;
- *Politique relative à la gestion et à la sécurité des actifs informationnels;*
- *Règlement relatif à l'utilisation des ressources informatiques et de télécommunications.*

3 DÉFINITIONS

Actif informationnel – Une information reçue ou produite par l'UQO, quel que soit son canal de communication (téléphone, réseau de télécommunication, voix, etc.) ou son support (papier, pellicule photographique ou cinématographique, ruban magnétique, support électronique, disque dur, etc.), un système ou une technologie de l'information.

Confidentialité – Propriété d'une information qui n'est accessible qu'aux personnes ou entités désignées et autorisées et qui n'est divulguée qu'à celles-ci.

Unités – Les unités d'enseignement, les unités de recherche et les unités administratives.

Utilisateur d'actifs informationnels – Toute personne, membre ou non de la communauté universitaire, qui utilise les ressources informatiques et de télécommunication de l'UQO.

4 CONFIGURATION

4.1. Configuration de l'ordinateur

Les appareils fournis par l'UQO sont gérés par la solution Microsoft Intune. Ces appareils sont chiffrés, comprennent un logiciel antivirus, maintien automatiquement les mises à jour de sécurité et permettre la suppression des données à distance en cas de perte ou de vol. L'altération des paramètres est interdite. Ceci assure la sécurité de votre ordinateur, de ses données et de l'intégrité du réseau de l'Université.

4.2. Connexion à Internet

Afin d'effectuer du télétravail, vous aurez besoin d'une connexion haute vitesse à Internet stable. Veuillez respecter les consignes suivantes :

- Utilisez une connexion Internet fiable;
- Évitez de vous connecter à des réseaux sans-fil publiques, inconnus ou ouverts;
- Assurez-vous que votre réseau sans fil soit sécuritaire et protégé par un mot de passe.

5 GESTION DES ACTIFS INFORMATIONNELS

5.1 Actifs informationnels numériques

- Assurez-vous de protéger les données sensibles disponibles à partir de votre ordinateur en limitant l'accès à celui-ci par un mot de passe et en verrouillant l'accès lorsque vous ne l'utilisez pas;
- Utilisez les systèmes et accédez aux actifs informationnels dans le respect des accès qui vous sont accordés.
- Classez, **sur vos partages réseau ou en infonuagique sur Microsoft 365 de l'UQO (Teams pour les documents d'équipe et OneDrive pour vos documents personnels)**, tout document et dossier créé dans des outils autres dès que cela est possible. L'objectif est de centraliser les documents administratifs de l'UQO et d'en permettre le partage et l'accès à vos collègues, tout en assurant leur intégrité;
- Les outils tels que Teams, OneDrive et SharePoint sont considérés comme des espaces pouvant contenir les versions officielles des fichiers si les procédures sont en place dans votre secteur (direction, service, département ou module). Si aucune procédure n'est en place pour votre secteur, les fichiers officiels doivent être sauvegardés sur les serveurs de l'UQO, soit dans votre dossier personnel (U) ou dans un dossier partagé (P);
- Lorsque vous utilisez un outil infonuagique, privilégiez l'envoi d'un lien vers les documents plutôt que de joindre celui-ci dans un courriel (voir guide d'utilisation d'un partage de fichiers avec OneDrive et voir les formations vidéos pour Teams. Cela aura un effet minimal sur la bande passante de l'Université en plus de diminuer les multitudes de copies et versions des documents;
- Protégez les renseignements personnels ou sensibles. Assurez-vous de les déposer ou de les partager dans un endroit sécuritaire (ex. : OneDrive et Teams) si vous devez les partager à des collègues en dehors de l'UQO. Si vous devez envoyer un document sensible par courriel, minimalement, sécurisez-le avec un mot de passe et acheminez le mot de passe dans un courriel distinct;
- Lorsque vous téléchargez des documents, ceux-ci se retrouvent dans le dossier de téléchargements de votre ordinateur. Afin d'éviter que des informations sensibles soient laissées dans ce dossier, nous vous recommandons de détruire ceux-ci lorsque vous avez terminé de les consulter.

5.2 Actifs informationnels papier

- La personne cadre responsable de l'unité administrative doit déterminer quels sont les types de documents qui peuvent être transportés entre le lieu de travail et le lieu de télétravail. Pour connaître les meilleures pratiques en matière de circulation des documents, nous vous invitons à écrire au Service des archives et de gestion des documents à l'adresse suivante : archives@uqo.ca.
- Toute personne qui fait du télétravail doit conserver les documents dans des conditions d'entreposage qui garantissent leur sécurité ainsi que la protection des données confidentielles

et des renseignements personnels, conformément à *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*. La destruction des documents papier contenant ce type d'information doit être effectuée par déchiquetage uniquement. Si la personne faisant du télétravail ne dispose pas d'une déchiqueteuse à son domicile ou d'une pièce ou un classeur pouvant être verrouillés, elle doit rapporter les documents confidentiels à protéger ou à détruire à l'Université lors des heures d'ouverture.

6. UTILISATION D'ORDINATEURS ET D'APPAREILS MOBILES

Afin de vous permettre d'effectuer efficacement du télétravail, l'UQO vous offre diverses possibilités.

6.1 Utilisation d'un ordinateur portable avec réseau virtuel privé (VPN)

Cette option est possible que pour les **ordinateurs fournis par l'UQO et intégrer à la solution de gestion Microsoft Intune**. Ceci vous permettra de vous brancher au réseau de l'UQO comme si vous étiez sur place. Vous pourrez accéder à vos fichiers partagés et à certaines applications non disponibles à l'extérieur du réseau de l'UQO. Pour ce faire, vous devrez faire une requête au Service des technologies de l'information (STI). Lorsque votre requête sera approuvée, il vous suffira de suivre la procédure de branchement qui vous sera transmise.

Lorsque vous utilisez le VPN de l'UQO, il est essentiel d'adopter les bonnes habitudes suivantes :

- Utilisez un **ordinateur de l'UQO** seulement;
- Utilisez le VPN seulement lorsque vous avez besoin d'accéder à des systèmes qui ne sont pas accessibles directement par Internet;
- Redoublez de vigilance lorsque la connexion est active : votre poste devient une porte d'entrée vers le réseau interne de l'UQO;
- Évitez de naviguer sur des sites Internet sans lien avec votre travail pendant que votre connexion VPN est active;
- Désactivez votre connexion dès qu'elle n'est plus nécessaire. Vous permettrez ainsi à d'autres collègues de se brancher sans encombrer le réseau;
- Les connexions VPN peuvent être journalisées surveillées pour des raisons de sécurité.

6.2 Utilisation de la solution de bureau à distance virtuel (VDI)

L'utilisation de la solution VDI permet d'accéder à un ordinateur virtuel de façon sécuritaire à partir d'un ordinateur personnel. Voici les équipements et configurations minimales pour l'utilisation de cette solution :

- Connexion Internet haute vitesse stable;
- Ordinateur ou tablette personnelle récente;
- Effectuer les mises à jour dès leurs disponibilités;
- Avoir un antivirus à jour[1];
- Afin de pouvoir utiliser efficacement les logiciels de vidéoconférence (Zoom et Teams), l'ordinateur devra avoir une Webcam ainsi qu'un micro et haut-parleur. Les logiciels devront être installés sur l'ordinateur et non sur l'ordinateur virtuel pour permettre une meilleure communication;
- Désactivez votre connexion dès qu'elle n'est plus nécessaire. Vous permettrez ainsi à d'autres collègues de se brancher sans encombrer le réseau.

[1] L'UQO ne fournit pas d'antivirus pour les ordinateurs personnels

L'utilisation de la solution VDI n'est que pour les personnes faisant du télétravail occasionnel. Si vous avez une entente de télétravail régulière[2], un ordinateur portable de l'UQO vous sera fournis et viendra remplacer votre ordinateur de bureau.

6.3 Chiffrement et verrouillage

Les appareils mobiles doivent être chiffrés pour protéger l'Université en cas de perte ou de vol. Lorsque l'option est disponible, activez le chiffrement sur vos appareils mobiles (téléphones, portables, etc.). Assurez-vous d'utiliser un mot de passe pour accéder à votre ordinateur ainsi qu'à votre téléphone portable. Activez aussi le verrouillage automatique après un délai d'inactivité. Veuillez ne pas sauvegarder de documents qui pourraient contrevenir à la *Directive relative à l'entreposage des actifs informationnels.*

7 UTILISATION DU COURRIEL

7.1 Tentatives d'hameçonnage

Redoublez de vigilance et soyez à l'affût des potentielles tentatives d'hameçonnage que vous pourriez recevoir par courriel ou par SMS. Rappelez-vous que l'UQO ne vous demandera jamais d'informations personnelles par courriel telles que : votre nom d'utilisateur et votre mot de passe, votre date de naissance ou votre numéro d'assurance sociale. Veuillez vous référer à la Directive encadrant la déclaration des courriels d'hameçonnage.

7.2 Courriel de l'UQO

Le courriel institutionnel **@uqo.ca** est un actif informationnel de l'UQO. Afin de ne pas mettre en péril la sécurité des informations qui sont transmises par courriel, veuillez ne pas configurer de règle de transfert automatique vers vos comptes personnels (Gmail ou autre).

7.3 Échanges d'informations

Si vous devez échanger des informations ou des documents avec vos collègues ou avec des étudiantes et étudiants, vous devez utiliser le courriel institutionnel **@uqo.ca** et protéger les documents confidentiels par un mot de passe, le cas échéant. Les adresses courriel personnelles ne sont pas sécurisées et l'échange d'information nominative ou sensible engendre des risques ; leur utilisation est donc interdite dans le cadre de vos fonctions.

8 OBLIGATION DE RESPECTER LE GUIDE D'UTILISATION

8.1 Formation

Tout membre du personnel désirant faire du télétravail devra suivre et avoir réussi les formations annuelles mises en place dans le cadre de la *Politique gouvernementale en cybersécurité*. Le programme de formation sera communiqué à tous les membres du personnel dès qu'il sera disponible.

[2] Entente de télétravail régulière = 2 jours et plus par semaine

8.2 Procédure de dénonciation

Toute personne qui a des motifs raisonnables et probables de croire qu'une utilisation non conforme à ce guide a été commise ou est en voie d'être commise doit, dès que possible, aviser le Service des technologies de l'information et lui fournir tous les renseignements et tous les documents disponibles et pertinents.

8.3 Contrôle et vérification

Le Service des technologies de l'information se réserve le droit de vérifier la conformité à ce guide avec des utilisateurs d'actifs informationnels et les unités concernées, conformément à l'article 8.1 du *Règlement relatif à l'utilisation des ressources informatiques et de télécommunication*.

8.4 Sanctions

L'utilisateur d'actif informationnel qui contrevient aux dispositions de ce guide se verra refuser la poursuite du télétravail, automatiquement et sans appel.