Exigences de sécurité relatives à l'utilisation d'Office 365

Encadrements de sécurité

Direction Responsabilité sociale et innovation

Version: 14 octobre 2022

100-2045, rue Stanley, Montréal QC H3A 2V4
Tél. : 514-879-1793 / 1-800-263-1793
www.cnq.org

TABLE DES MATIÈRES

1. INTRODUCTION

L'objectif de ce document d'encadrement est de définir et normaliser les exigences minimales de sécurité requises pour l'utilisation d'Office 365 par un notaire de manière à favoriser la protection des renseignements personnels qu'il détient, conformément à l'article 5.1 de la Directive de Sécurité - Fournisseurs de services d'externalisation aux notaires de la Chambre et aux lois applicables en la matière. Il appartient toutefois au notaire de s'assurer qu'Office 365 convient à ses besoins et de l'utiliser de façon adéquate.

Notez toutefois que Office 365 est une solution changeante : Microsoft y apporte des ajustements régulièrement ! Dans le cas où ces exigences s'avèrent inexactes ou périmées, le notaire est invité à le soulever par l'entremise de l'adresse courriel techno@cnq.org. Il contribuera ainsi à faire de ce guide un outil vivant bénéficiant à toute la communauté notariale.

2. DÉFINITIONS

MFA : L'authentification multifacteur est une méthode d'authentification électronique dans laquelle un utilisateur est autorisé à accéder qu'après avoir présenté avec succès deux éléments de preuve ou plus à un mécanisme d'authentification.

3. EXIGENCES

Cette section présente les exigences obligatoires à respecter :

# Réf.	Exigences
O365-1.1	**Localisation des données** au Canada
O365-1.2	L'identifiant de chaque utilisateur doit être unique. De plus, l'utilisateur possédant plusieurs comptes doit choisir des **mots de passe différents** pour chacun d'entre eux.
O365-1.3	Configurer l'authentification – multifacteur (**MFA**) de Office 365.
O365-1.4	Configurer l'expiration des mots de passe des utilisateurs à **90 jours**, délai de bonne pratique mais qui peut-être supérieur selon les directives de votre organisation.
O365-1.5	Mettre en place un processus qui assure que, dès le **départ d'un employé,** son compte utilisateur est supprimé. Microsoft indique : Après avoir supprimé un utilisateur, l'administrateur a jusqu'à 30 jours pour restaurer le compte. **Note** : si vous souhaitez conserver l'information de l'employé, déplacez les données vers un autre emplacement AVANT de supprimer le compte.
O365-1.6	Configurer le **verrouillage** d'un compte après 10 tentatives de connexion infructueuses
O365-1.7	Effectuer une **sauvegarde quotidienne** des documents, la sauvegarde peut être dans un autre emplacement infonuagique, au Canada, différent de celui utilisé par Office 365, ou sur une solution de sauvegarde dans les bureaux du notaire.

# Réf.	Exigences
O365-1.8	Le notaire doit protéger la confidentialité de ses communications. Outlook permet de **chiffrer des courriels**, c'est-à-dire de convertir le texte brut et lisible du message, en un texte brouillé, chiffré. Seul le destinataire qui possède la clé peut déchiffrer le message. Une clé peut dans certains cas prendre la forme d'un mot de passe. Pour rappel, la communication du mot de passe doit toujours se faire séparément du message principal. Le chiffrement pourrait être utilisé pour tout envoi de données confidentielles à une adresse externe à l'étude.

4. RECOMMANDATIONS

Cette section présente des recommandations ayant pour but d'orienter le notaire et son fournisseur de service dans les choix à faire. Le notaire qui fait appel aux services d'un tel fournisseur doit s'en remettre à ce dernier à titre de référence principale ou pour toutes questions concernant son environnement propre.

# Réf.	Exigences
O365-2.1	Version minimale à acquérir : **Business Premium** d'Office 365
O365-2.2	Chaque administrateur doit avoir un **compte d'utilisateur personnel** et un **compte d'administrateur** : le premier pour les opérations quotidiennes, le second pour effectuer des fonctions administratives seulement.
O365-2.3	Utiliser la fonctionnalité **Inspecteur de document**, dans Word, Excel ou PowerPoint pour vérifier la présence des données masquées ou d'informations personnelles dans les métadonnées du fichier (c'est à dire les propriétés), afin d'éviter de divulguer tout élément confidentiel.
O365-2.4	Fournir une **formation** sur l'utilisation sécuritaire de Office 365 aux utilisateurs
O365-2.5	Activer les fonctionnalités d'Office 365 pour la protection contre les **logiciels malveillants** et l**ogiciel rançonneur.**
O365-2.6	**Empêcher** le transfert automatique de courriels vers l'extérieur de l'organisation
O365-2.7	Dans le cas d'utilisation de SharePoint, OneDrive ou Microsoft Teams, **activer** la protection contre les fichiers attachés malicieux.
O365-2.8	Activer les fonctionnalités *Microsoft Defender pour Office 365* contre l'hameçonnage via des liens web malicieux.

5. RÉFÉRENCES

2019_08_16_CNQ_tableau_lois_PRP.pdf

Formations Microsoft 365 pour petites les entreprises

Comparatif des versions de Microsoft 365

10 principales façons de sécuriser vos données Microsoft 365

National Cyber Awareness System

CIS Microsoft 365 Security Benchmark