

5 ASTUCES POUR PRÉSERVER LA CONFORMITÉ DES COMMUNICATIONS DE VOS ÉQUIPES

Phil Britt

La pandémie de COVID-19 contraint de nombreuses entreprises à opter pour le télétravail. Au-delà de grandes sociétés telles qu'Amazon, Apple, Google, Twitter, Iron Mountain et Airbnb, des entreprises qui n'avaient jamais auparavant envisagé le télétravail demandent ou imposent à ceux de leurs collaborateurs qui le peuvent de travailler depuis chez eux.

Si les bureaux de la plupart des entreprises sont dotés de systèmes qui garantissent la sécurité et la conformité des communications de leurs collaborateurs, ces protections ne sont pas toujours déployées pour les télétravailleurs en cette période de pandémie de COVID-19.

Voici cinq astuces pour préserver la conformité de vos communications d'entreprise lorsque vos collaborateurs travaillent depuis chez eux pour se mettre à l'abri de la maladie.

1. VÉRIFIEZ L'ARCHIVAGE AUTOMATISÉ DES COMMUNICATIONS

Les secteurs réglementés, les services financiers par exemple, sont régis par des lois spécifiques qui imposent un archivage bien précis des communications. Bien que les secteurs non réglementés n'aient pas les mêmes contraintes, il est judicieux de s'assurer que les protocoles établis par l'entreprise sont respectés. Cependant, comme le souligne un article du blog [JD Supra](#) l'archivage des communications exige davantage qu'un simple paramétrage d'un système dont on ne se soucie plus ensuite. Il vous faut superviser l'archivage automatisé pour vous assurer que rien ne lui échappe.

2. PROTÉGEZ-VOUS CONTRE LES FUITES DE DONNÉES

Il est probable que les télétravailleurs iront sur les réseaux sociaux, lesquels sont faciles à compromettre. Comme l'a rapporté [BBC News](#), des comptes Facebook ont été temporairement piratés en février. Utilisez des solutions logicielles qui génèrent des alertes automatiques en cas de risques de sécurité potentiels pour les publications sur les réseaux sociaux.

3. VÉRIFIEZ QUE LES SOLUTIONS DE COMMUNICATION FONCTIONNENT BIEN SUR DIFFÉRENTS ÉQUIPEMENTS

Vous aurez beau fournir d'excellents équipements d'entreprise à vos collaborateurs, ça ne les empêchera probablement pas d'utiliser également leurs propres appareils. C'est pourquoi tant d'entreprises ont adopté des politiques BYOD (« apportez votre équipement personnel ») sur le lieu de travail. Il est



recommandé d'utiliser une infrastructure de bureau virtuel, un anti-virus et d'autres logiciels de protection et de définir des politiques claires quant à l'utilisation des équipements personnels à des fins professionnelles.

4. UTILISEZ DES SOLUTIONS CONFORMES AUX RÉGLEMENTATIONS MONDIALES

De nombreuses entreprises ont des activités à l'étranger et aux États-Unis. Choisir des solutions de communication qui assurent la conformité à la LPRDE, dispositions générales Règlement sur la protection des données (RGPD) ainsi que les réglementations américaines et autres réglementations mondiales.

5. CONSULTEZ UN EXPERT

Vérifier la sécurité et la conformité des collaborateurs qui passent d'un environnement interne à l'entreprise à un environnement de télétravail total ou hybride (à distance et sur site donc) peut s'avérer une tâche ardue. Prenez conseil auprès d'un expert pour établir les bonnes pratiques de sécurité de l'information pour votre entreprise.

PROTÉGER CE QUI COMPTE LE PLUS^{MD}

800.899.IRON | [IRONMOUNTAIN.CA/FR](https://ironmountain.ca/fr)



À PROPOS D'IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM) est un important fournisseur de services de stockage et de gestion des renseignements. Grâce à son réseau immobilier de plus de 67 millions de pieds carrés s'étendant à 1 000 installations dans 36 pays, l'entreprise peut répondre aux clients partout dans le monde. De plus, ses solutions pour la gestion des dossiers, des données, des documents et des centres de données ainsi que pour le déchiquetage protégé aident les organisations à réduire leurs coûts de stockage, à se conformer aux règlements, à se rétablir d'une catastrophe et à mieux utiliser leurs renseignements. Fondée en 1951, Iron Mountain stocke et protège des milliards d'actifs informationnels, y compris des documents commerciaux, des bandes de sauvegarde, des fichiers électroniques et des données médicales. Pour plus d'information, visitez le www.ironmountain.ca/fr

© 2020 Iron Mountain Canada Operations ULC. Tous droits réservés. La raison sociale Iron Mountain et le logo figurant une montagne sont des marques de commerce ou des marques déposées d'Iron Mountain Incorporated aux États-Unis et dans d'autres pays et leur usage par Iron Mountain Canada Operations ULC est autorisé. Toutes les autres marques de commerce ou marques déposées sont la propriété de leurs détenteurs respectifs.