IRON MOUNTAIN®

BONNES PRATIQUES EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION ET DE RECORDS MANAGEMENT POUR LES TÉLÉTRAVAILLEURS

« IL EST IMPORTANT DE RAPPELER À NOS COLLABORATEURS EN MODE TÉLÉTRAVAIL LES BONNES PRATIQUES DE GESTION ET DE SÉCURITÉ DE L'INFORMATION. SACHANT QUE DANS LES PÉRIODES DIFFICILES LES PERSONNES ONT TENDANCE À ADOPTER DES SOLUTIONS DE CONTOURNEMENT. VEILLEZ À MAINTENIR UNE COMMUNICATION SIMPLE ET SPÉCIFIQUE. »

ARLETTE WALLS

Responsable Monde de la Gestion des documents et de l'information chez Iron Mountain (Iron Mountain, Global Records & Information Manager)

Les entreprises du monde entier sont confrontées à de nouveaux défis exceptionnels liés à la pandémie de COVID-19. À l'heure où tant de collaborateurs sont en mode télétravail, Iron Mountain partage les bonnes pratiques pour préserver la sécurité et la confidentialité de vos informations pendant cette période sans précédent.

Que vous travailliez dans un bureau à cloisons ou modulaire ou bien chez vous, la gestion des documents et des données répond aux mêmes règles : les politiques de l'entreprise doivent être respectées par tous les collaborateurs. Parce que le contexte actuel est propice à des questions et inquiétudes diverses pendant toute la durée de la crise, les collaborateurs ont besoin d'une communication claire et d'un rappel des politiques et des procédures.

POLITIQUES

Veillez à ce que tous vos collaborateurs puissent accéder aux politiques. Rappelez-leur où elles sont disponibles sur votre intranet. Communiquez-les à l'ensemble de vos collaborateurs. Dans le doute, reportez-vous aux politiques pour :

- Le Records Management et la gestion de l'information
- La sécurité
- La confidentialité
- Les recommandations du service RH en matière de télétravail
- La sécurité des équipements, et notamment :
  - l'utilisation acceptable des équipements et le traitement de l'information
  - la copie de documents sur un équipement personnel
  - l'envoi de documents vers une adresse de messagerie personnelle
  - les pilotes de l'imprimante du domicile
  - l'utilisation de clés USB

N'oubliez pas d'indiquer des coordonnées pour répondre à toute question et inquiétude.

SÉCURITÉ

En situation de télétravail, les collaborateurs doivent être extrêmement vigilants concernant la sécurité de l'information et des équipements.

- Protégez vos équipements contre tout accès non autorisé en les rangeant de manière sécurisée lorsqu'ils ne sont pas en service.
- Ne partagez ni les équipements ni vos identifiants et mots de passe avec les personnes qui vivent avec vous.
- Enregistrez tout le contenu sur votre réseau désigné et non pas sur votre poste de travail.
  - Les informations sauvegardées sur votre poste de travail ne sont ni stockées ni protégées de manière sécurisée.
- Évitez d'imprimer des archives/documents.
- Si vous devez absolument imprimer, veillez à la sécurité de ces documents comme suit :
  - Ne jetez pas les archives/documents papier de votre entreprise à la poubelle ou dans le bac de recyclage.

- Gardez les documents imprimés en lieu sûr jusqu'à ce que vous puissiez :
    1. Revenir au bureau et détruire ces documents dans un broyeur sécurisé.
    2. Les détruire avec votre broyeur personnel, conformément à la politique de broyage mise en place par votre entité.
    3. Vous rendre chez un prestataire qui propose des services de destruction sécurisée des documents.
- Que vous travailliez chez vous ou dans un lieu public (en respectant les consignes liées au COVID-19), utilisez une connexion sécurisée plutôt qu'une connexion WiFi publique.
- Utilisez un filtre de confidentialité pour écran afin de protéger vos informations.
- Apprenez à vos collaborateurs à faire preuve d'hypervigilance par rapport aux cyberattaques, ransomware et aux emails d'hameçonnage (phishing). Prévenez-les que des criminels cherchent à exploiter la propagation du coronavirus pour lancer des cyberattaques et des campagnes de piratage.

CONFIDENTIALITÉ

En cas de traitement/d'utilisation de documents contenant des données personnelles, vous devez respecter scrupuleusement les exigences de conformité et ces informations ne doivent pas être communiquées à des personnes non autorisées.

Il est crucial que les données privées et sensibles, ainsi que la propriété intellectuelle, ne soient exposées à aucun risque potentiel de violation ou de détournement.

NOUS PROTÉGEONS CE QUI A LE PLUS DE VALEUR POUR VOUS®

0800 215 218 | IRONMOUNTAIN.FR

À PROPOS D'IRON MOUNTAIN

Iron Mountain Incorporated (NYSE : IRM) est un spécialiste mondial des solutions de conservation et de gestion de l'information qui aide les entreprises à réduire les coûts, les risques et les inefficacités liés à la gestion de leurs données physiques et digitales. Fondée en 1951, Iron Mountain stocke et protège des milliards d'actifs informationnels, parmi eux des données de sauvegarde ou archivées, des fichiers électroniques et fournit notamment des services de numérisation et de destruction sécurisée à des entreprises du monde entier. Pour en savoir plus, rendez-vous sur www.ironmountain.fr