FICHE D'INFORMATION

Check-list de sécurité des données pour l'intégration des nouveaux collaborateurs

Avez-vous récemment accueilli de nouveaux collaborateurs dans votre organisation ? Si tel est le cas, il est essentiel d'aborder la question de la sécurité des informations dès le début.

Une erreur ou la négligence d'un collaborateur est l'une des principales causes des violations de données et une formation approfondie peut contribuer grandement à atténuer les risques. Les responsables et les équipes de direction peuvent contribuer à créer et à renforcer la culture de sécurité d'une entreprise en définissant des stratégies et en veillant à ce que les collaborateurs reconnaissent leur rôle dans la protection des données.

LE SAVIEZ-VOUS ?

Près de la moitié (49 %) des chefs d'entreprise interrogés indiquent que le manque de compréhension des menaces et des risques pour l'organisation est le principal obstacle au respect des politiques de sécurité de l'information par les collaborateurs.[1]

Voici une checklist des sujets relatifs à la sécurité des informations, tant électroniques que sur papier, à passer en revue lors de l'intégration.

☐ **Règlement sur la sécurité de l'information.**
Les violations de données peuvent entraîner des amendes et nuire à la réputation d'une entreprise. Le fait de familiariser les employés avec les principaux aspects des lois sur la sécurité des données peut fournir un cadre idéal pour les discussions importantes sur la sécurité des données.

☐ **Signalement d'incident.**
Malgré tous les efforts d'une entreprise, une violation de données peut toujours se produire. Les employés doivent savoir quand et comment signaler ces événements et être assurés qu'ils ne seront pas pénalisés pour avoir parlé. Veillez à informer vos nouveaux employés des pratiques et des attentes en matière de signalement des incidents dès le départ, afin que les nouveaux employés et les anciens comprennent comment réagir si une violation de données devait se produire.

☐ **Procédures d'impression.**
Les erreurs courantes, comme laisser par inadvertance des documents confidentiels en évidence dans des endroits tels que les imprimantes, augmentent le risque de violation des données. Il est essentiel de souligner l'importance de récupérer rapidement les documents imprimés au niveau de l'imprimante, car cela peut réduire la probabilité de vol d'informations. Si votre entreprise protège ses imprimantes par un mot de passe, n'oubliez pas de former les nouveaux employés sur la manière d'accéder à ces mots de passe et d'en préserver la sécurité.

☐ **Politiques relatives aux appareils électroniques.**
Les téléphones mobiles personnels et les tablettes sur le lieu de travail sont pratiques, mais ils peuvent présenter un risque accru d'incidents de sécurité. Lors de l'intégration des nouveaux collaborateurs, assurez-vous qu'ils comprennent comment protéger leurs appareils à tout moment.

Source : 1. ** Rapport 2021 sur la protection des données de Shred-it.

We protect what matters.

Shred-it®
A Stericycle® Solution

☐ Garder un bureau propre.

Si votre entreprise a une politique officielle de bureau propre, vous devez expliquer exactement ce que cela signifie pour les nouveaux collaborateurs. En général, les collaborateurs sont tenus de mettre sous clé tous les papiers contenant des informations confidentielles, de retirer les documents non essentiels du dessus du bureau et d'activer l'écran de verrouillage de l'ordinateur avant de partir pour une période prolongée ou à la fin de la journée.

Cliquez ici pour découvrir la notre politique de bureau propre.

☐ Élimination complète des documents.

Les nouveaux collaborateurs doivent bien comprendre comment éliminer correctement les documents de votre entreprise. Informer les nouveaux collaborateurs de vos procédures existantes d'élimination des documents peut contribuer à atténuer les risques et à limiter les complications liées à la protection des données. Il peut être préférable d'instaurer une politique de d'élimination complète Shred-it All et de leur conseiller de mettre tous les documents dans une console sécurisée afin de garantir une destruction sûre. Ainsi, vous n'aurez plus à vous demander ce qui peut être confidentiel ou non. Non seulement cela contribue à la sécurité des documents confidentiels, mais comme tout le papier déchiqueté est recyclé, c'est aussi une bonne pratique en termes de durabilité.

Cliquez ici pour découvrir notre politique Shred-it ALL.

☐ Protocoles pour les mots de passe.

Les mots de passe sont une mesure de sécurité essentielle. Les nouveaux collaborateurs doivent être pleinement informés de la politique de votre organisation en matière de mots de passe et savoir ce que signifie « générer des mots de passe forts ». Un bon mot de passe comprend des lettres majuscules et minuscules, des chiffres et des symboles, et doit être mis à jour régulièrement. Si votre entreprise dispose d'un programme de mise à jour obligatoire des mots de passe, assurez-vous que les nouveaux collaborateurs en sont informés.

☐ Précautions pour les e-mails.

Les incidents de cybersécurité surviennent souvent parce que les collaborateurs cliquent sur des e-mails qu'ils ne devraient pas. Les nouveaux collaborateurs doivent être formés à la reconnaissance des e-mails suspects, y compris les logiciels malveillants, les tentatives de hameçonnage et les rançongiciels, afin qu'ils puissent apprendre à éviter les situations dangereuses.

Pour en savoir plus sur les bonnes pratiques concernant la sécurité des informations, consultez shredit.fr ou appelez le 0800 844 848

Nous protégeons ce qui compte.

Shred-it®
Une Solution Stericycle®