FICHE CONSEIL SUR LA SÉCURITÉ DES DONNÉES DANS LE CADRE DE LA GESTION DES DONNÉES OPÉRATIONNELLES

CENTRE DE DONNÉES HUMANITAIRES D'OCHA

CartONG a assuré la traduction de cette fiche conseil, grâce au soutien de CLEAR Global et du ministère français de l'Europe et des Affaires étrangères.

INTRODUCTION

La sécurité des données est un élément clé de la responsabilité en matière de données: la gestion sécurisée, éthique et efficace des données en vue d'une réponse opérationnelle. Elle implique un ensemble de mesures physiques, technologiques et procédurales qui protègent la confidentialité, l'intégrité et la disponibilité des données et empêchent leur perte, leur destruction, leur altération, leur acquisition ou leur divulgation accidentelles ou intentionnelles, illégales ou non autorisées de quelque manière que ce soit.

Cette fiche conseil propose une série d'actions recommandées pour la sécurité des données dans le cadre de la gestion des données opérationnelles. Ces actions doivent être mises en œuvre conformément aux mandats institutionnels, aux politiques et aux cadres juridiques et réglementaires applicables.

ADOPTEZ DE BONNES PRATIQUES DE GESTION DES MOTS DE PASSE

- Sécurisez vos appareils et vos comptes à l'aide de mots de passe forts comprenant des chiffres, des lettres majuscules et minuscules, des symboles et au moins 16 caractères par mot de passe.
- Activez l'authentification multifacteurs pour tous les comptes.
- Ne réutilisez pas le même mot de passe pour plusieurs comptes.
- Ne stockez pas vos mots de passe physiquement (par exemple sur des post-its) ou numériquement (dans un fichier sur votre appareil) et ne partagez pas votre mot de passe avec d'autres personnes.
- N'activez pas la fonction "Se souvenir de moi" dans les applications et les navigateurs.
- Changez immédiatement les mots de passe de vos comptes en ligne en cas de perte ou de vol de votre appareil.

UTILISEZ UN LOGICIEL ANTIVIRUS/ANTI-MALWARE

- Assurez-vous que vos appareils sont équipés d'un logiciel antivirus/anti-malware adéquat.
- Si vous avez des questions sur les outils adéquats ou sur la manière de les configurer, consultez le spécialiste informatique de votre bureau.

MAINTENEZ LES LOGICIELS ET LES SYSTÈMES D'EXPLOITATION À JOUR

- Vérifiez régulièrement que votre appareil, vos logiciels, vos applications et les plug-ins de votre navigateur sont à jour et activez les mises à jour automatiques de votre système d'exploitation.
- Utilisez des navigateurs web tels que Chrome ou Firefox qui reçoivent des mises à jour de sécurité automatiques.
- Éteignez vos appareils à la fin de la journée pour permettre les mises à jour et vous protéger contre les attaques.

ÉVITEZ LES ESCROQUERIES PAR HAMEÇONNAGE ET FAITES ATTENTION À CE SUR QUOI VOUS CLIQUEZ

- Lorsque vous recevez des courriels ou des messages suspects, vérifiez toujours l'adresse ou les coordonnées de l'expéditeur et ne cliquez sur les liens ou les pièces jointes que si vous avez confiance en l'expéditeur.
- Ne répondez pas aux courriels suspects et ne les transmettez pas à vos collègues.
- Signalez toute activité suspecte à votre équipe d'assistance informatique.

UTILISEZ LES APPAREILS MOBILES DE MANIÈRE RESPONSABLE

- Dans la mesure du possible, utilisez des appareils spécifiques pour le travail. Conservez en permanence vos appareils professionnels dans un endroit sûr et évitez de les trimbaler inutilement.
- Utilisez des outils de messagerie validés par votre organisation et qui offrent un cryptage de bout en bout.
- Désactivez ou réduisez au minimum la connectivité Bluetooth.
- Utilisez un réseau privé virtuel (VPN) validé par votre organisation lorsque vous travaillez en ligne. Déconnectez-vous toujours de votre/vos compte(s) si vous utilisez un ordinateur ou un appareil partagé.
- Désactivez les fonctions de déverrouillage biométrique, en particulier lorsque vous êtes en transit.

PROTÉGEZ LES DONNÉES SENSIBLES ET MINIMISEZ LES DONNÉES

- Tenez **un registre des traitements de données** qui indique le niveau de sensibilité de chaque type de données géré par votre bureau. Révisez régulièrement les niveaux de sensibilité en fonction de l'évolution du contexte.
- Ne collectez que la quantité minimale de données nécessaires pour atteindre l'objectif et les finalités d'une activité particulière de gestion de données.
- Ne conservez les données sensibles que le temps nécessaire à la réalisation de l'objectif pour lequel elles sont traitées et conformément aux directives, lois et réglementations applicables.
- Transférez et stockez les données à l'aide d'outils et de canaux validés par votre organisation (localement sur un serveur ou un ordinateur fixe ou portable de l'organisation ; ou sur des serveurs et des systèmes gérés à distance par le biais d'applications telles que OneDrive, SharePoint et Teams).
- Protégez par mot de passe les fichiers (Word, Excel, PDF) contenant des données sensibles et partagez les mots de passe des documents par des canaux distincts (par exemple, envoyez par SMS un mot de passe pour un document envoyé par courriel).
- Limitez et contrôlez soigneusement le nombre de personnes ayant accès aux données sensibles.
- Définissez un calendrier de conservation et de destruction pour toutes les données gérées et utilisez des outils adéquats pour la destruction des données.
- Cryptez vos courriels.

RESSOURCES CLÉS

- **Lignes directrices opérationnelles du IASC sur la responsabilité en matière de données dans le cadre de l'action humanitaire**
- **Note d'orientation sur la gestion des incidents liés aux données**
- **Fiche de conseils sur l'utilisation responsable des outils de conférence en ligne**

*Pour en savoir plus sur la gestion des données sensibles dans les opérations humanitaires, consultez la page **Responsabilité des données** sur le site web du Centre ou contactez notre équipe à l'adresse **centrehumdata@un.org**.*