KIT CADRE · MODULE 4 · RENFORCER SA SÉCURITÉ

Plan de sécurité

Mon entreprise

Une liste de contrôle pour les mots de passe, les copies et les fraudes, et ce qu'il faut faire si quelque chose arrive. Remplissez ce plan pendant la pratique du module R · Renforcer sa sécurité.

R
CADRE

COMMENT L'UTILISER

1. **Cochez ce qui est vraiment en place.** Pour le reste, indiquez qui s'en occupe et pour quand.
2. **Remplissez le protocole avant d'en avoir besoin.** Gardez-en une copie imprimée ou hors ligne.
3. **Revoyez ce plan** à chaque départ d'employé, changement d'outil ou incident.
4. **N'écrivez ici aucun mot de passe et aucune donnée personnelle de clients.**

Liste de contrôle

	Comptes et accès	Qui	Pour quand
☐	Un mot de passe différent pour la messagerie, la banque et le paiement mobile.		
☐	Des mots de passe longs, gardés dans un endroit protégé.		
☐	La double vérification est activée sur la messagerie et les comptes d'argent.		
☐	Chaque personne a son propre accès ; il est retiré le jour de son départ.		
☐	Téléphones et ordinateurs se verrouillent avec un code.		

	Copies de sauvegarde	Qui	Pour quand
☐	Je sais quels fichiers sont indispensables.		
☐	Ces fichiers existent en deux copies, dont une hors de l'entreprise.		
☐	La fréquence des copies est fixée.		
☐	J'ai déjà ouvert un fichier à partir de la copie pour vérifier qu'elle fonctionne.		

Cofinanciado por la Unión Europea

	Fraudes	Qui	Pour quand
☐	Personne ne communique un code reçu par message, même à un prétendu service technique.		
☐	Un paiement est confirmé dans le compte lui-même, jamais sur une capture d'écran.		
☐	Tout changement de coordonnées de paiement est vérifié par un numéro déjà connu.		
☐	Un message urgent qui demande de ne consulter personne est traité comme suspect.		
☐	Avant d'accorder un accès, je vérifie qui le demande et ce que j'accorde.		

	Données des clients	Qui	Pour quand
☐	Je sais quelles données je garde, où, et pour quoi faire.		
☐	Je vérifie qui peut ouvrir mes liens de partage.		
☐	Je ne mets dans un outil d'IA que des données nécessaires à la tâche et autorisées.		
☐	Mes clients sont informés quand je recueille leurs données ; pas de promotion par messagerie sans leur accord préalable.		
☐	J'ai vérifié mes démarches selon la loi n° 2017-020 : déclaration auprès de l'APD ou consentement écrit.		

Ce dont chaque tâche a vraiment besoin :

Groupe de données	Type d'information	Nécessaire pour cette tâche ?	Ce que je fais et pourquoi
Noms et contacts			
Factures et paiements (MRU)			
Notes particulières (santé, situation)			
Données du personnel			

Protocole en cas d'incident

Un incident n'est pas seulement un piratage : c'est aussi un accès non autorisé, une modification, une perte ou une destruction. **Un simple soupçon suffit pour agir et prévenir.**

1. **Arrêter.** Stoppez les envois, chargements et accès liés au problème. Ne poursuivez pas la conversation suspecte pour « enquêter ».
2. **Limiter.** Faites ce qui est prévu et permis : retirer un lien que vous avez créé, changer un mot de passe.
3. **Prévenir tout de suite.** Un message court au responsable suffit ; n'attendez pas de tout savoir.
4. **Conserver les traces.** N'effacez ni conversation, ni fichier, ni registre pour cacher ce qui s'est passé.
5. **Séparer les faits et les suppositions.** Dites ce que vous savez, ce que vous ignorez, ce qui est fait et ce qui est en attente.
6. **Laisser décider.** Le responsable évalue les risques et décide s'il faut informer les clients ou l'Autorité de protection des données (APD).
7. **Reprendre seulement après vérification.**

Situation	Premier geste	Qui j'appelle
Compte piraté	Changer le mot de passe et déconnecter les appareils et sessions inconnus.	
Téléphone perdu ou volé	Bloquer la ligne et les comptes d'argent auprès de l'opérateur.	
Fraude au paiement mobile	Ne rien renvoyer ; noter l'heure, le montant en MRU et la référence ; contacter l'opérateur.	
Fichiers perdus ou bloqués	Isoler l'appareil, ne rien payer, repartir de la dernière copie vérifiée.	
Données de clients exposées	Retirer l'accès si c'est permis, prévenir le responsable, conserver les traces.	

Mes contacts utiles :

Rôle	Nom ou service	Comment le joindre
Responsable des décisions		
Appui technique		
Banque		
Opérateur de paiement mobile		
Autorité de protection des données (APD)		

FICHE D'INCIDENT (À COPIER POUR CHAQUE INCIDENT)

Date et heure de détection : .....

Outil ou compte concerné : .....

Ce qui s'est passé (faits) : .....

Ce que je ne sais pas encore : .....

Fichiers ou catégories de données touchés : .....

Montant concerné (MRU) : .....

Actions faites / demandées / en attente : .....

Personne prévenue et heure : .....

Décision et retour à la normale : .....

Faire relire votre plan par le tuteur IA

Copiez ce texte dans le **tuteur IA** du campus, remplacez la dernière ligne par votre plan, puis envoyez-le.

À COPIER DANS LE TUTEUR IA

Voici mon plan de sécurité pour la pratique du module Renforcer sa sécurité.
Vérifie ces critères un par un. Pour chacun, indique « respecté » ou « à améliorer », avec une phrase d'explication.
Ne réécris pas mon travail et ne donne pas de note.
1. Les comptes clés de l'entreprise sont identifiés.
2. La copie de sauvegarde existe et a été testée.
3. Il y a une règle claire pour vérifier les demandes et les paiements.
4. Le protocole dit qui prévient qui.
5. Aucun secret n'est écrit dans le plan.
MON TRAVAIL : [collez ici votre plan]

Le tuteur IA est une aide automatisée : il ne certifie pas votre conformité à la loi n° 2017-020. Vérifiez ses remarques, puis décidez vous-même des corrections.

BLOC DE CONTINUITÉ · R

Décidé : .....

En attente : .....

Version enregistrée : .....

Prochaine étape : .....