

Checklist

Employeur



Accompagner
vos
collaborateurs



1 Gardez votre charte informatique à jour

- Revoir les règles BYOD (apporter votre propre appareil) et intégrer des recommandations pour le travail à domicile.
- Prendre en compte les risques liés aux réseaux Wi-Fi publics et expliquer aux collaborateurs comment se connecter en toute sécurité en dehors des locaux de l'entreprise.
- Mettre à jour les règlements et chartes concernant l'impression, le stockage et la destruction des documents papier (au bureau comme à domicile).
- Renforcer les consignes concernant les mots de passe (MFA, etc.).
- Exiger l'effacement sécurisé de toutes les données avant la mise au rebut du matériel informatique.

2 Former régulièrement vos équipes

- Former les employés aux bases du RGPD, à la gestion des données et aux six principes de la protection des données.
- Inclure des modules sur la gestion des documents papier sensibles et les règles de conservation.
- Ajouter des formations sur la sécurité des documents en télétravail.
- Utiliser une plateforme de formation en ligne.
- Fournir des outils pratiques tels qu'une checklist ou une auto-évaluation « Bilan santé et sécurité des données »
- Intégrer la NIS2 dans les formations comme un niveau complémentaire de cybersécurité, en particulier pour les équipes IT.

3 Équiper correctement les employés

- Fournir des PC d'entreprise plutôt que de compter sur les appareils personnels (BYOD).
- Investir dans des antivirus et pare-feu performants.
- Garantir l'accès à des destructeurs de documents : modèles professionnels au bureau et destructeurs compacts à domicile.
- Utiliser des destructeurs à coupe micro (P-5) pour les données hautement confidentielles.
- Prioriser les fonctionnalités liées à la productivité et à la sécurité (ex. prévention des bourrages, utilisation sécurisée).

4 Communiquer fréquemment

- Renforcer la sécurité à tous les niveaux et accompagner les collaborateurs les moins expérimentés.
- Intégrer la thématique de la sécurité des données dans les réunions et entretiens individuels.
- Diffuser les mises à jour des règlements et chartes via des affiches, des newsletters et l'intranet.
- Partager régulièrement des alertes sur le phishing et les cyberattaques.
- Faire de la sécurité des données un point permanent dans les revues d'activité trimestrielles.
- Positionner le RGPD comme socle de conformité, et NIS2 pour renforcer la culture de cybersécurité.

Checklist Employé



La sécurité des données au quotidien



1 Protégez vos données numériques

- Utilisez des mots de passe forts et uniques, stockés dans un gestionnaire de mots de passe.
- Activez l'authentification à deux facteurs.
- Méfiez-vous du phishing, ne cliquez pas sur des liens ou pièces jointes suspects.
- Gardez vos appareils à jour, protégés par un mot de passe et avec un antivirus actif.
- Utilisez toujours le VPN de l'entreprise lorsque vous travaillez à distance et évitez le Wi-Fi public.
- Respectez les règles de l'entreprise si vous utilisez des appareils personnels (BYOD).

2 Gérer correctement les documents papier sensibles

- Identifiez les données sensibles : informations personnelles, dossiers d'entreprise, fichiers RH, documents financiers.
- Détruisez les documents une fois les délais de conservation atteints (ex. contrats, dossiers RH, reçus, relevés).
- Ne laissez pas traîner de documents papier – videz votre bureau chaque jour et rangez-les sous clé.
- Réfléchissez avant d'imprimer – imprimez uniquement si nécessaire.
- Détruisez les documents sensibles avant de les jeter, ne les mettez jamais directement à la poubelle.
- Passez régulièrement en revue les documents stockés et anonymisez les données personnelles quand c'est possible.

3 Respectez les chartes internes et suivez les formations

- Suivez régulièrement les formations obligatoires et les modules de remise à niveau.
- Sensibilisez vos collègues si vous observez un comportement à risque.
- Maîtrisez les six principes de la protection des données.
- En cas de doute sur le règlement ou la gestion des données, adressez-vous à votre manager ou à votre délégué à la protection des données.
- Restez à jour sur les chartes internes et les lois en matière de protection des données, y compris NIS2.