

# Évaluer le niveau de sécurité des données personnelles de votre organisme

Avez-vous pensé à ?

Fiche		Mesure	
1	Sensibiliser les utilisateurs	Informez et sensibilisez les personnes manipulant les données	<input type="checkbox"/>
		Rédigez une charte informatique et lui donner une force contraignante	<input type="checkbox"/>
2	Authentifier les utilisateurs	Définissez un identifiant ( <i>login</i> ) unique à chaque utilisateur	<input type="checkbox"/>
		Adoptez une politique de mot de passe utilisateur conforme à nos recommandations	<input type="checkbox"/>
		Obligez l'utilisateur à changer son mot de passe après réinitialisation	<input type="checkbox"/>
		Limitez le nombre de tentatives d'accès à un compte	<input type="checkbox"/>
3	Gérer les habilitations	Définissez des profils d'habilitation	<input type="checkbox"/>
		Supprimez les permissions d'accès obsolètes	<input type="checkbox"/>
		Réaliser une revue annuelle des habilitations	<input type="checkbox"/>
4	Tracer les accès et gérer les incidents	Prévoyez un système de journalisation	<input type="checkbox"/>
		Informez les utilisateurs de la mise en place du système de journalisation	<input type="checkbox"/>
		Protégez les équipements de journalisation et les informations journalisées	<input type="checkbox"/>
		Prévoyez les procédures pour les notifications de violation de données à caractère personnel	<input type="checkbox"/>
5	Sécuriser les postes de travail	Prévoyez une procédure de verrouillage automatique de session	<input type="checkbox"/>
		Utilisez des antivirus régulièrement mis à jour	<input type="checkbox"/>
		Installez un « pare-feu » ( <i>firewall</i> ) logiciel	<input type="checkbox"/>
		Recueillez l'accord de l'utilisateur avant toute intervention sur son poste	<input type="checkbox"/>
6	Sécuriser l'informatique mobile	Prévoyez des moyens de chiffrement des équipements mobiles	<input type="checkbox"/>
		Faites des sauvegardes ou synchronisations régulières des données	<input type="checkbox"/>
		Exigez un secret pour le déverrouillage des smartphones	<input type="checkbox"/>
7	Protéger le réseau informatique interne	Limitez les flux réseau au strict nécessaire	<input type="checkbox"/>
		Sécurisez les accès distants des appareils informatiques nomades par VPN	<input type="checkbox"/>
		Mettez en œuvre le protocole WPA2 ou WPA2-PSK pour les réseaux Wi-Fi	<input type="checkbox"/>

8	Sécuriser les serveurs	Limitez l'accès aux outils et interfaces d'administration aux seules personnes habilitées	<input type="checkbox"/>
		Installez sans délai les mises à jour critiques	<input type="checkbox"/>
		Assurez une disponibilité des données	<input type="checkbox"/>
9	Sécuriser les sites web	Utilisez le protocole TLS et vérifiez sa mise en œuvre	<input type="checkbox"/>
		Vérifiez qu'aucun mot de passe ou identifiant ne passe dans les url	<input type="checkbox"/>
		Contrôlez que les entrées des utilisateurs correspondent à ce qui est attendu	<input type="checkbox"/>
		Mettez un bandeau de consentement pour les <i>cookies</i> non nécessaires au service	<input type="checkbox"/>
10	Sauvegarder et prévoir la continuité d'activité	Effectuez des sauvegardes régulières	<input type="checkbox"/>
		Stockez les supports de sauvegarde dans un endroit sûr	<input type="checkbox"/>
		Prévoyez des moyens de sécurité pour le convoyage des sauvegardes	<input type="checkbox"/>
		Prévoyez et testez régulièrement la continuité d'activité	<input type="checkbox"/>
11	Archiver de manière sécurisée	Mettez en œuvre des modalités d'accès spécifiques aux données archivées	<input type="checkbox"/>
		Détruisez les archives obsolètes de manière sécurisée	<input type="checkbox"/>
12	Encadrer la maintenance et la destruction des données	Enregistrez les interventions de maintenance dans une main courante	<input type="checkbox"/>
		Encadrez par un responsable de l'organisme les interventions par des tiers	<input type="checkbox"/>
		Effacez les données de tout matériel avant sa mise au rebut	<input type="checkbox"/>
13	Gérer la sous-traitance	Prévoyez une clause spécifique dans les contrats des sous-traitants	<input type="checkbox"/>
		Prévoyez les conditions de restitution et de destruction des données	<input type="checkbox"/>
		Assurez-vous de l'effectivité des garanties prévues (audits de sécurité, visites, etc.)	<input type="checkbox"/>
14	Sécuriser les échanges avec d'autres organismes	Chiffrez les données avant leur envoi	<input type="checkbox"/>
		Assurez-vous qu'il s'agit du bon destinataire	<input type="checkbox"/>
		Transmettez le secret lors d'un envoi distinct et via un canal différent	<input type="checkbox"/>
15	Protéger les locaux	Restreignez les accès aux locaux au moyen de portes verrouillées	<input type="checkbox"/>
		Installez des alarmes anti-intrusion et vérifiez-les périodiquement	<input type="checkbox"/>
16	Encadrer les développements informatiques	Proposez des paramètres respectueux de la vie privée aux utilisateurs finaux	<input type="checkbox"/>
		Évitez les zones de commentaires ou encadrez-les strictement	<input type="checkbox"/>
		Testez sur des données fictives ou anonymisées	<input type="checkbox"/>
17	Utiliser des fonctions cryptographiques	Utilisez des algorithmes, des logiciels et des bibliothèques reconnues	<input type="checkbox"/>
		Conservez les secrets et les clés cryptographiques de manière sécurisée	<input type="checkbox"/>