ÉVALUER LE NIVEAU DE SÉCURITÉ DES DONNÉES PERSONNELLES DE VOTRE ORGANISME

Avez-vous pensé à ?

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

ÉVALUER LE NIVEAU DE SÉCURITÉ DES DONNÉES PERSONNELLES DE VOTRE ORGANISME

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