Objet du marché : .....

Numéro de la consultation : .....

Le titulaire doit prendre toutes les précautions utiles au regard des risques présentés par son traitement pour préserver la séc
soient déformées, endommagées ou que des tiers non autorisés y aient accès.
En particulier, il est invité, pour l'exécution du marché :
- à préciser, s'il mettra en oeuvre les mesures suivantes,
- sinon, à justifier de la mise en place de mesures équivalentes ou de leur absence de nécessité ou de possibilité :

Catégories	Code mesure	Mesure
Sensibiliser les utilisateurs	PAS-01	Informer et sensibiliser les personnes manipulant les données
	PAS-02	Rédiger une charte informatique et lui donner une force contraignante
Authentifier les utilisateurs	PAS-03	Définir un identifiant (login) unique à chaque utilisateur
	PAS-04	Adopter une politique de mots de passe utilisateur conforme aux recommandations de la CNIL
	PAS-05	Obliger l'utilisateur à changer son mot de passe après réinitialisation
	PAS-06	Limiter le nombre de tentatives d'accès à un compte
Gérer les habilitations	PAS-07	Définir des profils d'habilitation
	PAS-08	Supprimer les permissions d'accès obsolètes
	PAS-09	Réaliser une revue annuelle des habilitations
Tracer les accès et gérer les incidents	PAS-10	Prévoir un système de journalisation
	PAS-11	Informer les utilisateurs de la mise en place du système de journalisation
	PAS-12	Protéger les équipements de journalisation et les informations journalisées
	PAS-13	Prévoir les procédures pour les notifications de violation de données à caractère personnel
Sécuriser les postes de travail	PAS-14	Prévoir une procédure de verrouillage automatique de session
	PAS-15	Utiliser des antivirus régulièrement mis à jour
	PAS-16	Installer un «pare-feu» (firewall) logiciel
	PAS-17	Recueillir l'accord de l'utilisateur avant toute intervention sur son poste
Sécuriser l'informatique mobile	PAS-18	Prévoir des moyens de chiffrement des équipements mobiles
	PAS-19	Faire des sauvegardes ou des synchronisations régulières des données
	PAS-20	Exiger un secret pour le déverrouillage des ordiphones
Protéger le réseau informatique interne	PAS-21	Limiter les flux réseau au strict nécessaire
	PAS-22	Sécuriser les accès distants des appareils informatiques nomades par VPN
	PAS-23	Mettre en oeuvre le protocole WPA2 ou WPA2-PSK, ou supérieur, pour les réseaux Wi-Fi
Sécuriser les serveurs	PAS-24	Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées
	PAS-25	Installer sans délai les mises à jour critiques
	PAS-26	Assurer une disponibilité des données
Sécuriser les sites web	PAS-27	Utiliser le protocole TLS et vérifier sa mise en oeuvre
	PAS-28	Vérifier qu'aucun mot de passe ou identifiant n'est encapsulé dans les URL
	PAS-29	Contrôler que les entrées des utilisateurs correspondent à ce qui est attendu
	PAS-30	Mettre un bandeau de consentement pour les cookies et autres traceurs non nécessaires au service
Sauvegarder et prévoir la continuité d'activité	PAS-31	Effectuer des sauvegardes régulières
	PAS-32	Stocker les supports de sauvegarde dans un endroit sûr
	PAS-33	Prévoir des moyens de sécurité pour le convoyage des sauvegardes

	PAS-34	Prévoir et tester régulièrement la continuité d'activité
Archiver de manière sécurisée	PAS-35	Mettre en oeuvre des modalités d'accès spécifiques aux données archivées
	PAS-36	Détruire les archives obsolètes de manière sécurisée
Encadrer la maintenance et la destruction des données	PAS-37	Enregistrer les interventions de maintenance dans une main courante
	PAS-38	Encadrer par un responsable de l'organisme les interventions par des tiers
	PAS-39	Effacer les données de tout matériel avant sa mise au rebut
Gérer la sous-traitance	PAS-40	Les relations avec les prestataires qui traitent des données au nom et pour le compte du responsable de traitement (l'organisme employeur) doivent faire l'objet d'un accord écrit. Cet accord doit contenir une ou des clauses spécifiques relatives aux obligations respectives des parties résultant du traitement des données à caractère personnel. L'accord doit notamment prévoir les conditions de restitution et de destruction des données. Il incombe au responsable de traitement de s'assurer de l'effectivité des garanties prévues (audits de sécurité, visites, etc.). Pour plus de précisions, vous pouvez vous reporter au guide de la sous-traitance et aux exemples des clauses de sous- traitance.
Sécuriser les échanges avec d'autres organismes	PAS-41	Ne pas transmettre des fichiers contenant les données à caractère personnel des usagers en clair via des messageries grand public
	PAS-42	Privilégier des moyens de communication autres que les messageries grand public pour communiquer des informations relatives aux personnes accompagnées à d'autres travailleurs sociaux ou organismes (p. ex.: plateformes d'échanges sécurisées, messagerie interne, etc.)
	PAS-43	Chiffrer les pièces sensibles à transmettre, si cette transmission utilise la messagerie électronique
	PAS-44	S'assurer qu'il s'agit du bon destinataire
	PAS-45	Assurer la confidentialité des secrets (clé de chiffrement, mot de passe, etc.) en les transmettant via un canal distinct (par exemple, envoi du fichier chiffré par courriel et transmission du secret par téléphone ou par SMS
Protéger les locaux et les bureaux physiques	PAS-46	Restreindre les accès aux locaux au moyen de portes verrouillées
	PAS-47	Installer des alarmes anti-intrusion et les vérifier périodiquement
	PAS-48	Ranger tous les documents papiers relatifs aux usagers dans des armoires fermées à clé
	PAS-49	Verrouiller la porte d'accès au bureau en cas d'absence prolongée
Encadrer les développements informatiques	PAS-50	Proposer des paramètres respectueux de la vie privée aux utilisateurs finaux
	PAS-51	Encadrer de manière stricte les zones de commentaires libres
	PAS-52	Tester sur des données fictives ou anonymisées
Utiliser des fonctions cryptographiques	PAS-53	Utiliser des algorithmes, des logiciels et des bibliothèques reconnus
	PAS-54	Conserver les secrets et les clés cryptographiques de manière sécurisée
Sécuriser les mots de passe des usagers	PAS-55	Utiliser un gestionnaire de mots de passe ou un carnet stocké dans un coffre-fort pour enregistrer les mots de passe des usagers accompagnés dans le cadre de l'accompagnement numérique
Sécuriser les données de santé	PAS-56	En cas d'hébergement des données de santé à caractère personnel réalisé pour le compte des organismes assurant le suivi social ou médico-social par un prestataire informatique, celui-ci doit être agréé ou certifié pour l'hébergement, le stockage, la conservation de données de santé, conformément aux dispositions de l'article L. 1111-8 du code de la santé publique.

.....

:urité des données et, notamment au moment de leur collecte, durant leur transmission et leur conservation, empêcher qu'elles

Réponse de l'entreprise (menu déroulant)	Observations complémentaires et justifications
