POLITIQUE DE SÉCURITÉ
DES DONNÉES PERSONNELLES

Mesures de protection des données — Règlement (UE) 2016/679 — Référentiel PSDM (HAS)

IDENTIFICATION DU DOCUMENT			
Référence	POL-SECU-001	**Version**	V1
Date de création	27 mai 2026	**Date de révision**	
Rédacteur (DPO / RAQ)	Roman BASSET, DPO	**Approbateur**	Ghislain JANSÉ, président
Périodicité de revue	Annuelle ou suite événement de sécurité significatif		
Direction, DPO / DPD, RAQ, Responsable IT, Ensemble des collaborateurs			

OBJET PRÉSENTATION ET PORTÉE DU DOCUMENT

La présente politique définit l'ensemble des mesures techniques et organisationnelles mises en œuvre par J'M SANTÉ pour garantir la sécurité, la confidentialité et l'intégrité des données personnelles traitées dans le cadre de ses activités, conformément au Règlement Général sur la Protection des Données (RGPD — Règlement (UE) 2016/679), à la Loi Informatique et Libertés modifiée et au référentiel de certification PSDM (HAS).

Elle s'applique à l'ensemble des collaborateurs, sous-traitants et prestataires ayant accès aux systèmes d'information et aux données de la structure. Le respect de cette politique est obligatoire et constitue une condition de l'exercice des fonctions au sein de J'M SANTE

1 CONTRÔLES D'ACCÈS ET AUTHENTIFICATION

La maîtrise des accès aux systèmes d'information et aux données personnelles constitue le premier niveau de protection. Les mesures suivantes sont mises en œuvre :

- Mise en place de mots de passe robustes (longueur minimale, complexité, renouvellement périodique) pour tous les comptes utilisateurs
- Authentification forte à double facteur (2FA / MFA) obligatoire pour les accès aux systèmes sensibles (logiciel métier, messagerie professionnelle, accès à distance)
- Gestion stricte des droits d'accès selon le principe du moindre privilège : chaque utilisateur n'accède qu'aux données strictement nécessaires à sa fonction
- Procédure formalisée d'attribution, de modification et de révocation immédiate des accès (notamment en cas de départ d'un collaborateur)
- Journalisation des accès aux systèmes et aux données sensibles, et surveillance régulière des connexions

2 PROTECTION PHYSIQUE ET ENVIRONNEMENTALE

La sécurité physique des locaux et des infrastructures est un préalable indispensable à la protection des données numériques :

- Sécurisation des locaux et des zones d'archives contenant des documents à caractère personnel ou confidentiel
- Accès restreint et contrôlé aux salles serveurs et aux espaces contenant des équipements informatiques critiques
- Les clés des magasins sont confiés à 8 personnes identifiées
- Destruction sécurisée des documents papier contenant des données personnelles (broyage, prestataire agréé DASRI pour les dossiers médicaux) dans les deux magasins

3 SÉCURISATION DES POSTES DE TRAVAIL

Chaque poste de travail constitue un point d'entrée potentiel pour les cybermenaces. Les mesures suivantes s'appliquent à l'ensemble des équipements informatiques de la structure :

- Verrouillage automatique des sessions après une période d'inactivité (délai maximum : 10 minutes)
- Protection antivirus et anti-malware installée et maintenue à jour sur tous les postes
- Interdiction de stockage local non autorisé de données sensibles (dossiers patients, données RH) en dehors des espaces sécurisés définis
- Mises à jour régulières des systèmes d'exploitation et des logiciels (correctifs de sécurité)
- Sauvegarde régulière des données critiques selon la règle 3-2-1 (3 copies, 2 supports différents, 1 hors site) (logiciel métier G5 en hébergement sur site)
- Charte informatique signée par chaque collaborateur lors de son entrée en fonction

4 SÉCURISATION DES RÉSEAUX ET COMMUNICATIONS

La sécurisation des échanges de données entre les différents systèmes et acteurs est essentielle pour prévenir les interceptions et les accès non autorisés :

- Segmentation du réseau interne pour limiter la propagation d'une éventuelle attaque
- Filtrage des accès Internet et blocage des ports non utilisés via pare-feu configuré et maintenu à jour
- Surveillance en temps réel et systèmes de détection des intrusions (alarmes)
- Interdiction d'utiliser des réseaux Wi-Fi publics non sécurisés pour accéder aux systèmes de la structure

5 CHIFFREMENT ET ANONYMISATION

Le chiffrement des données garantit leur confidentialité même en cas d'accès non autorisé aux supports ou aux flux de communication :

- Anonymisation ou pseudonymisation des données lorsque les finalités du traitement le permettent (statistiques, études, bases de test)
- Chiffrement systématique des supports amovibles (clés USB, disques durs externes) utilisés pour le transport de données sensibles
- Prévoir la mise en place d'un système de sauvegarde interne.(cloud type Google DRIVE)
- Chiffrement des emails contenant des données personnelles ou médicales lors de transmissions externes (à mettre en place)

6 GESTION DES INCIDENTS DE SÉCURITÉ

Tout incident de sécurité susceptible d'affecter des données personnelles doit être signalé, analysé et traité dans les meilleurs délais, conformément à la procédure de gestion des violations de données (Réf. PROC_RGPD-001) :

- Mise en place d'une procédure formalisée de gestion, de qualification et de notification des incidents de sécurité
- Signalement immédiat au DPO par tout collaborateur ayant constaté ou suspecté un incident
- Journalisation systématique des incidents, analyse des causes racines et documentation des mesures correctives
- Déclaration à la CNIL dans les 72 heures si l'incident constitue une violation de données personnelles (Art. 33 RGPD)

- Communication interne et externe planifiée, validée par la Direction, en cas de violation avérée
- Retour d'expérience (REX) systématique après chaque incident significatif

7 SENSIBILISATION ET FORMATION DU PERSONNEL

La sécurité des données repose en grande partie sur les comportements individuels. L'ensemble des collaborateurs est formé et sensibilisé de manière régulière :

- Formation initiale à la sécurité informatique et à la protection des données lors de l'intégration de tout nouveau collaborateur
- Formation annuelle de recyclage sur les évolutions réglementaires et les nouvelles menaces (cybersécurité, ingénierie sociale)
- Sensibilisation aux bonnes pratiques : détection de l'hameçonnage (phishing), gestion des mots de passe, confidentialité des dossiers patients
- Exercices de simulation (ex. : fausse campagne de phishing) pour évaluer le niveau de vigilance
- Traçabilité des formations : attestations archivées dans le dossier de chaque collaborateur

8 SÉCURISATION DES RELATIONS AVEC LES SOUS-TRAITANTS

Tout sous-traitant ou prestataire ayant accès aux données personnelles de la structure est soumis aux mêmes exigences de sécurité, conformément à l'Art. 28 RGPD :

- Vérification préalable des engagements de sécurité et de conformité RGPD des prestataires avant toute contractualisation
- Signature obligatoire d'un contrat de traitement de données (DPA) incluant des clauses spécifiques de sécurité, de confidentialité et de notification des incidents
- Interdiction contractuelle de sous-traitance ultérieure sans accord préalable du J'M SANTÉ
- Suivi régulier des prestataires critiques (revue annuelle, questionnaires de sécurité, audits le cas échéant)
- Clause de réversibilité et de destruction des données à la fin du contrat

9 SAUVEGARDES ET CONTINUITÉ D'ACTIVITÉ

La disponibilité et la récupérabilité des données en cas d'incident sont garanties par un dispositif de sauvegarde et de continuité rigoureux :

- Sauvegardes automatisées et quotidiennes de l'ensemble des données critiques (dossiers patients, données RH, données de facturation)
- Application de la règle 3-2-1 : 3 copies des données, sur 2 supports différents, dont 1 hors site (cloud sécurisé ou site de secours physique)
- Tests périodiques de restauration (au minimum trimestriels) pour vérifier l'intégrité des sauvegardes
- Plan de continuité d'activité (PCA) et plan de reprise d'activité (PRA) formalisés, testés et mis à jour annuellement
- Identification des systèmes et données critiques et définition des objectifs de temps de reprise (RTO) et de point de reprise (RPO)

10 CONFORMITÉ ET REVUE PÉRIODIQUE

La politique de sécurité des données est un document vivant, révisé régulièrement pour tenir compte des évolutions légales, technologiques et organisationnelles :

- Revue annuelle de l'ensemble des politiques et des mesures de sécurité par le DPO et le Responsable IT, avec présentation à la Direction
- Mise à jour du document dès que nécessaire : évolution légale ou réglementaire, incident de sécurité significatif, changement d'infrastructure
- Audits internes de sécurité annuels et audits externes périodiques (tests d'intrusion, audit RGPD)
- Suivi des indicateurs de sécurité : nombre d'incidents, délais de détection, taux de personnel formé, résultats des tests de restauration
- Intégration des conclusions des audits et des REX dans le plan d'actions qualité de la structure

ENGAG. ENGAGEMENT DE LA DIRECTION

La Direction de J'M SANTÉ s'engage à mettre à disposition les ressources humaines, techniques et financières nécessaires à la mise en œuvre et au maintien de la présente politique de sécurité des données.

Le respect de cette politique est obligatoire pour l'ensemble des collaborateurs et des sous-traitants. Tout manquement est susceptible d'entraîner des mesures disciplinaires ou contractuelles adaptées.

	La Direction générale
Roman BASSET, DPO le 16/06/2026 Signature : Roman BASSET Roman BASSET JM SANTE 253, Bd Robert Roch 34500 BEZIERS Tél. : 04 67 01 35 78	Ghislain JANSÉ, président le 16/06/2026 Signature : Ghislain JANSE J'M SANTE 253 bd Robert Koch Immeuble Le Rubans 34500 BEZIERS Tel. : 04 67 01 35 78 SIRET 34 795 950 00029 - APE 7010 Z

Seule la version en vigueur disponible dans le système documentaire qualité fait foi.
Document à diffuser à l'ensemble des collaborateurs et à joindre à la charte informatique.