

Annexe Suite logicielle Teranga Software

Version 1.0 – Avril 2025

Préambule

Cette annexe Suite logicielle Teranga Software, ci-après “Conditions Particulières”, vient compléter les informations présentes dans les CGV annexées à la Proposition Commerciale.

Elle vient préciser les conditions et les traitements en lien avec la Suite logicielle Teranga souscrite et s’applique de plein droit.

Teranga Software (ci-après “ Le Prestataire”) est éditeur d’une Suite logicielle : NETContact, NETFactu, NETPlanning, NETSoins et NETVie (ci-après la « Suite logicielle »), sans que cette liste ne soit limitative, qui permet au Client de pouvoir administrer les données de leurs usagers.

Toutes dispositions dérogeant aux présentes CGV et à cette annexe devront résulter d’un accord exprès des Parties, reflété dans la Commande confirmée par le Prestataire ou tout autre document faisant foi de l’accord des deux Parties.

1. Conditions financières

Les montants facturés seront libellés en euros et seront payés dans cette monnaie.

Tous les prix indiqués dans le contrat et ses annexes sont indexés pour toute la durée du contrat conformément aux CGV transmises avec la Proposition Commerciale.

1.1. Durée et reconduction

Le Contrat est conclu par les Parties pour une durée de quarante-huit (48) mois « Période initiale » à compter de la date de signature de la VSR par le Client ou le premier jour de déploiement effectif (dernier jour de la formation initiale), sauf autre accord précisé à la Proposition Commerciale.

Après la Période Initiale, les contrats sont renouvelés tacitement et annuellement, sauf résiliation adressée 3 mois avant la date anniversaire en LRAR, soit avant le 30 septembre.

La Période initiale ou la Période renouvelée concernée sera ci-après dénommée la « Période ».

En cas de dénonciation du Contrat par le Client, aucun avoir ni aucun remboursement au titre de la Période ne seront consentis par le Prestataire.

1.2. Redevance récurrente

L'abonnement/maintenance payé par le Client est fixé dans la Proposition Commerciale. Il est défini sur une base annuelle au 1^{er} janvier, terme à échoir et fonction de la capacité de l'établissement du Client (nombre de lits ou d'usagers). Le Client s'engage à informer le Prestataire dans un délai de 30 jours de toute modification de cette capacité.

En cas de signature de Proposition Commerciale en cours d'année, l'abonnement/maintenance sera payé au prorata temporis pour l'année en cours à compter de la date du déploiement intégrant la formation initiale, puis au 1^{er} janvier les années suivantes.

L'abonnement/maintenance comprend :

- L'assistance
- La maintenance corrective des Progiciels souscrits
- L'hébergement des données du Client.

1.3. Prestation de formation

Le Prestataire fournit une prestation de formation sur ses Progiciels. La formation aux Progiciels est obligatoire pour un groupe de référents définis par l'établissement.

L'assistance technique téléphonique (hotline) n'est accessible qu'aux utilisateurs ayant suivi la formation.

Les formations, prévues au sein de la Proposition Commerciale et signées par le Client, sont planifiées d'un commun accord entre le Prestataire et le Client.

Toute journée de formation commandée est facturable.

Toute journée de formation planifiée qui est annulée ou reportée à l'initiative du Client sera facturée :

- Dans sa totalité, si l'annulation ou de report est formulée moins de 31 jours avant le 1^{er} jour de formation.
- À hauteur de 50%, si l'annulation ou de report est formulée entre 31 et 60 jours avant le 1^{er} jour de formation.

À ce jour, le Prestataire est certifié Qualiopi.

Un devis sera établi sur-mesure selon le nombre de participants et les spécificités de l'établissement.

Ces prestations peuvent être réalisées sur site ou à distance.

1.4. Autres prestations

Les prestations non définies dans la Proposition Commerciale donneront lieu , le cas échéant, à l'application des tarifs et conditions de règlements définis d'un commun accord entre les Parties selon la nature de la prestation concernée. Ces prestations complémentaires donneront lieu à une facture séparée.

Ces tarifs sont indexés pour toute la durée du contrat conformément aux CGV.

Dans le cas des prestations soumises à devis, le détail est précisé dans la Proposition Commerciale.

1.5. Modalités de réversibilité

Il est entendu entre les Parties que la mise en œuvre de la réversibilité ne suspend pas l'exécution des obligations contractuelles des Parties. Par conséquent, le Prestataire continuera de facturer au Client les Services au titre du Contrat, le Client s'engageant corrélativement à les honorer. La réversibilité ne pourra s'effectuer avant la date effective de fin de contrat afin de contenir toutes les données demandées.

Le Prestataire s'engage à fournir au Client un export dans un format structuré.

2. Condition d'accès ou pré-requis

Le Prestataire fournit à ses Clients la Suite logicielle en mode SaaS, c'est-à-dire un service hébergé en ligne et accessible via Internet.

Le Client devra prendre à ses frais toutes ses dispositions avec son FAI (Fournisseur d'accès internet) pour disposer d'une connexion Internet dotée des caractéristiques minimum suivantes :

- 1 MB de débit descendant
- 0.1 MB de débit montant
- 250 ms ping

Les prérequis sont disponibles sur demande et prévalent sur tout autre document.

Ils sont susceptibles d'évoluer selon les versions. Le Prestataire garantit le bon fonctionnement de sa Suite logicielle :

- sur le navigateur Google Chrome dans sa dernière version

- sur un système d'exploitation windows 64bits à jour et supporté par son éditeur (<http://windows.microsoft.com/fr-fr/windows/lifecycle>)
- avec une résolution minimale de l'écran : 1280 x 768
- L'application utilise des fichiers au format PDF 1.7 :
 - soit via le lecteur intégré à Google Chrome,
 - soit via un lecteur annexe tel que Adobe Reader

3. Hébergement & infogérance

Dans le cadre de l'hébergement qu'il assure, le Prestataire déploie une infrastructure redondée sur plusieurs centres de données géographiquement distincts, visant à garantir la confidentialité, l'intégrité et la disponibilité des informations.

Conformément à la législation, les informations nominatives hébergées ne sont communiquées qu'en cas de réquisition des autorités judiciaires ou dans d'autres situations prévues par la loi. Le Prestataire s'assure que toute manipulation de données respecte les obligations réglementaires, en particulier pour la protection des données personnelles.

Notre Partenaire Hébergeur s'engage à mettre en œuvre les moyens appropriés dans l'état de l'art pour veiller à la protection des serveurs hébergés.

Cette description est communiquée à titre indicatif. Elle pourra être mise à jour en fonction des avancées technologiques et des exigences opérationnelles. Le Prestataire s'engage toutefois à :

- Maintenir un niveau de performance technique et de sécurité au moins équivalent.
- Fournir ses prestations d'hébergement et d'infogérance en conformité avec les engagements convenus, y compris pour les mises à jour applicatives (cycle semestriel et déploiement continu de correctifs).

Toute évolution d'infrastructure sera réalisée de manière à préserver la continuité de service et la sécurisation des données.

Notre offre s'appuie sur un hébergeur agréé Hébergement de Données de Santé, dont la certification est consultable dans cette annexe. Cf. "Certifications & Labels"

Lorsque le Client importe et/ou stocke des données dans la Suite logicielle, il autorise le Prestataire et ses sous-traitants à procéder à l'hébergement, au stockage et à la reproduction de ces données, uniquement dans le but de fournir les Services. Cette autorisation reste valable pendant toute la durée du Contrat et

ne saurait servir à d'autres finalités que celles prévues (sauvegarde, mises à jour, maintenance).

Le Prestataire veille à respecter l'ensemble des obligations légales et réglementaires relatives à la protection des données sensibles.

3.1. DISPONIBILITÉ

Compte tenu de la nature des Services, Le Prestataire déploie ses meilleurs efforts pour maintenir la disponibilité et l'accessibilité du Progiciel au Client et s'engage à rétablir rapidement l'accès en cas de panne ou de dysfonctionnement. Le Prestataire peut, si nécessaire, interrompre l'accès au Progiciel notamment pour effectuer toutes opérations de sauvegarde des Données et/ou de maintenance de ses propres moyens matériels et logiciels utilisés pour assurer les prestations d'hébergement. Le Prestataire met à disposition du Client, sur simple demande de sa part, les plannings de maintenance de ses infrastructures.

Le Prestataire peut de surcroît effectuer une maintenance d'urgence interrompant temporairement l'exploitation afin de corriger des Anomalies et prévenir des atteintes aux Services imminentes. Cette maintenance d'urgence peut notamment résulter d'une constatation d'une faille de sécurité de nature à compromettre la sécurité des Services et les Données Client.

Disponibilité des services d'infrastructures à hauteur de 99,5 %.

3.2. SAUVEGARDES

Fréquence des sauvegardes : Les données sont sauvegardées quotidiennement sur des supports sécurisés avec une rétention de 12 mois.

Stockage des sauvegardes : Les sauvegardes sont externalisées et stockées dans des emplacements sécurisés, avec des copies hors site pour prévenir les risques physiques ou cyber.

Tests de restauration : Des tests de restauration sont effectués annuellement pour s'assurer que les données peuvent être récupérées en cas de besoin.

Les sauvegardes sont chiffrées pour garantir la confidentialité.

3.3. SÉCURITÉ ET CONFIDENTIALITÉ

Le Prestataire met en œuvre une politique de sécurité visant à contrôler les accès au Progiciel et à garantir la sécurité et la confidentialité des Données.

En cas de perturbations ou d'évènement susceptible d'affecter la sécurité des Données, Le Prestataire en informera le Client dans les plus brefs délais et prendra toutes mesures utiles pour rétablir les Services dans les meilleurs délais.

Notre prestataire hébergeur a mis en place des contrôles efficaces de protection contre l'accès physique non autorisé aux systèmes d'exploitation et aux applications, ainsi qu'aux renseignements confidentiels des Clients afin de procurer une assurance raisonnable que l'accès aux systèmes et aux Données des Clients est limité aux personnes autorisées et que les renseignements confidentiels des Clients sont protégés contre toute utilisation non conforme à leur usage.

Le site d'hébergement du Prestataire est totalement dédié sans circulation de personnel non habilité. Les accès à la salle sont complètement sécurisés, seul le personnel technique possédant les habilitations d'accès peut y entrer.

3.4. INTÉGRITÉ

Le Prestataire s'engage à mettre en place des contrôles efficaces de nature à procurer une assurance raisonnable que les applications mises à dispositions des Clients traitent les Données qui lui sont confiées sans risques d'omission, altération, déformation ou toutes autres formes d'anomalie susceptibles de nuire à l'intégrité des résultats issus de ces applications et que les traitements sont en conformité avec la réglementation légale qui leur sont applicables, et que les Données et traitements sont accessibles pour les contrôles et audits extérieurs qui pourraient être diligentés.

PCA/PRA: Le Prestataire a mis en place des Plans de Continuité d'Activité (PCA) et de Reprise d'Activité (PRA) afin d'assurer la disponibilité des services et la restauration des données en cas d'incident majeur

- Les sauvegardes sont réalisées quotidiennement sur des supports sécurisés avec une rétention adaptée aux besoins opérationnels
- Les données sont stockées de manière externalisée avec des copies hors site pour limiter les risques physiques ou cyber
- Des tests de restauration sont effectués régulièrement pour garantir la récupération des données en cas de besoin
- Les sauvegardes sont chiffrées afin d'assurer la confidentialité des informations stockées
- Un serveur de secours est disponible pour prendre le relais en cas d'incident et limiter les interruptions de service

4. Maintenance Progiciel & Support

L'abonnement/maintenance comprend les mises à jour de la Suite logicielle et des Services associés, l'assistance, la maintenance corrective de la Suite logicielle et l'hébergement des données du Client.

4.1. Maintenance

Le Prestataire assure la maintenance et la surveillance de la Suite logicielle de façon à permettre sa pérennité, le tout dans le cadre d'une obligation de moyen.

La maintenance porte uniquement sur les Progiciels souscrits auprès du Prestataire.

La prestation de maintenance corrective consiste en la correction de toute Anomalie qui apparaît dans l'utilisation de l'accès distant du Progiciel. Toute Anomalie identifiée par le Client doit être signalée au Prestataire.

Les demandes d'évolutions et d'adaptations pourront, après étude de faisabilité, être prises en charge et ajoutées par le prestataire dans une prochaine version.

Exclusions

Les prestations de maintenance fournies par Le Prestataire ne comportent pas la fourniture de nouvelles versions comportant des nouveaux modules, lesquels pourront, en revanche, faire l'objet d'un avenant au Contrat après accord des parties. Le Prestataire n'assurera pas le service de maintenance dans les cas suivants :

- utilisation de l'accès distant de manière non conforme à la documentation ;
- intervention non autorisée par le Client ou par un tiers ;
- anomalie générée par le matériel du Client ou ses équipements d'accès.

Le Prestataire n'assurera pas le service d'assistance corrective, ou pourra le cas échéant les assurer à des conditions financières à déterminer, dans les cas suivants :

- Changement des logiciels du constructeur implanté sur la configuration des postes de travail, difficilement, peu, ou non compatible avec le Progiciel objet du contrat de fourniture. À ce titre, les Parties conviennent de se tenir mutuellement informées d'un

éventuel changement, et Le Prestataire avertit le Client, des délais et des conditions de mise à niveau présumés ;

- Changement de tout ou partie du matériel compatible ou non compatible avec les Progiciels, objet des présentes, et non préalablement agréé par Le Prestataire ;
- Modification, révision, changement ou entretien du Progiciel par d'autres personnes que les préposés du Prestataire, sauf autorisation expresse écrite ;
- Exploitation sur le système du Client, par cette dernière ou par un tiers, de tout produit, programme (logiciels, progiciels) non fourni par Le Prestataire, et pouvant être à l'origine d'anomalies, du fait de ses interférences éventuelles avec le progiciel objet du présent contrat, mauvaise manipulation du Progiciel ;
- Tout événement assimilable à un cas de force majeure ou fait d'un tiers.

4.2. Support

Un Centre de Documentation est accessible depuis les Progiciels souscrits.

Il appartient aux utilisateurs de se reporter à cette Documentation avant chaque demande.

Avant de signaler un incident, le Client s'assure qu'il ne se situe pas sur ses équipements ou ceux sous sa responsabilité.

Le Client devra décrire de façon précise et exhaustive les symptômes du problème rencontré avant de les adresser.

Le niveau de gravité est établi d'un commun accord entre le Client et notre service support. En cas de désaccord, l'avis de ce dernier prévaudra jusqu'à éventuelle requalification entre les Parties.

Dans l'attente d'une solution définitive, Le Prestataire pourra préconiser une solution provisoire, dans les meilleurs délais compatibles avec la nature de la difficulté.

Modalités d'accueil du Support

Le Support est disponible du lundi au vendredi de 9h à 12h et de 14h à 18h hors jours fériés.

En cas d'urgence pour les applications santé, le support est disponible 24/7.

- contact depuis la suite logicielle
- contact téléphonique direct, répondeur, mail

Pour une réactivité optimale, le Client aura accepté et fait le nécessaire pour que les équipes techniques du Prestataire puissent intervenir à distance (télémaintenance via internet).

Prérequis

Le Support est ouvert uniquement au Client ayant accepté et signé le Contrat.
 Le Support est ouvert exclusivement aux Utilisateurs formés aux Progiciels.
 La hotline n'est disponible que pour la version de la Suite Logicielle la plus récente.

La réception par Le Prestataire de l'ensemble des informations requises à l'ouverture du ticket constitue le point de départ des délais de traitement de l'Anomalie.

4.3. Niveaux de services

Sur tout type de support, le délai de prise en compte d'un incident est de :

- 4H en cas d'incident majeur (utilisation impossible du Progiciel)
- 24H en cas d'incident mineur (gêne dans l'utilisation n'empêchant pas l'utilisation de la Suite Logicielle).

Sous réserve d'opérations de maintenance ou de suspension des Services conformément aux dispositions, le Prestataire s'engage à l'égard du Client, au respect, en dehors des périodes de maintenance programmées, des taux suivants :

- Disponibilité sur une base annuelle de la Suite Logicielle et des Services associés de 99,5% ;
- Garantie de temps d'intervention (GTI).

Une maintenance programmée d'1h nécessaire au maintien en condition opérationnelle de la plateforme est prévue chaque mois

*Heures ouvrées (HO) : lundi au vendredi de 9h à 18h

**Heures non ouvrées (HNO) : lundi au vendredi de 18h à 9h, le week-end et jours fériés.

Type	Description	Délais de prise en charge maximal (GTI)	
		HO*	HNO**
T1 - Bloquante	L'utilisation du logiciel est impossible Exemple : les serveurs ne répondent plus, problème sur une fonctionnalité critique (risque patient)	2h	4h
T2- Majeure	L'utilisation du logiciel est limitée, mais un	8h	48h

Type	Description	Délais de prise en charge maximal (GT)	
		HO*	HNO**
	contournement existe		
T3- Mineure	Dépannage quotidien Exemple : Paramétrage, aide à l'utilisation	72h	-
T4- Autre	Demande non prioritaire ou hors cadre	72h	-

Les T1 doivent être signalées via la ligne d'astreinte d'urgence afin de commencer à faire courir le délai de prise en charge.

Les astreintes, horaires non ouvrables, week-end et jours fériés ne traitent que les T1 et T2.

Les T3 et T4 seront traités dans les heures ouvrables.

Les T4 n'impliquent pas nécessairement une réponse ou un suivi

En cas de coupure de l'accès à l'initiative du Client ayant entraîné un déplacement sur site, ce déplacement ainsi que le temps passé seront facturés au Client, selon le tarif en vigueur pour une journée de prestation, auquel s'ajoutent les frais liés au déplacement.

Il est entendu que cette maintenance s'applique sur le code source non modifié de la Suite Logicielle. Toute modification par le Client du code source est interdite, et toute modification ayant entraîné un dysfonctionnement fera l'objet d'une correction facturable.

4.4. Connexion aux environnements Client

Dans le cadre des prestations de support et de maintenance, le Prestataire peut être amenée à se connecter ponctuellement à l'environnement de production du Client, exclusivement pour des besoins clairement identifiés tels que :

- le dépannage d'incident signalé via le support,
- les interventions urgentes liées à un dysfonctionnement critique,
- le contrôle de paramétrage technique à la demande du Client.

Ces accès sont strictement encadrés : ils sont réalisés via des connexions sécurisées et par du personnel habilité.

Ces accès sont journalisés et documentés dans les outils de support.

Le Client reconnaît autoriser ce type d'accès ponctuel en lien avec l'exécution du contrat. Aucun accès persistant n'est maintenu et aucune donnée n'est extraite hors du strict périmètre de l'intervention.

5. DESCRIPTION DES TRAITEMENTS DE DONNÉES

5.1. Traitements réalisés par Le Prestataire

Dans le cadre de la relation commerciale et contractuelle, Le Prestataire est amené à traiter des données personnelles de ses Clients et Collaborateurs en tant que Responsable de traitement.

Objet	Personnes concernées	Catégories Données	Sous-traitant & logiciel	Sécurité & garanties
Projet & échanges	Participant au projet, Direction, Administratif...	Identité, coordonnées de contact	Google Drive Messagerie Trello	Compte nominatif sécurisé par authentification Boîte mail sécurisée
Contrat et commandes	Participant au contrat ou au projet	Identité, coordonnées de contact	Google Drive Messagerie Universign/ DocuSign	Accès par compte nominatif sécurisé par authentification Boîte mail sécurisée Chiffrement
Comptabilité	Administratif Direction Commercial	Identité adresse mail	Sage, XRP CEGID Zeendoc	Accès par compte nominatif sécurisé par authentification
Newsletter & communication actualité	Clients, abonnés	Identité adresse mail	Mailjet Hubspot Brevo	Accès par compte nominatif sécurisé par authentification Clauses contractuelles type 2021 Chiffrement des données

5.2. Traitements Suite logicielle Teranga - sur instruction du Client

Pour les besoins de l'exécution du Contrat et notamment la réalisation des Services, le Prestataire est amené à traiter les Données des résidents pour le compte du Client.

Traitement	Finalité	Catégories Données	Sous-traitant	Transfert hors UE
Hébergement Suite logicielle	Mettre à disposition les Données nécessaires au fonctionnement des solutions pour nos Clients hébergés Réaliser les sauvegardes	Toutes les données de Suite logicielle Teranga et de connexion	CLARANET	Non
			AWS	Non
Dossier résident	Gérer l'accueil et les données administratives des résidents Gérer les projets et activité des résidents	Données d'identification Vie personnelle Situation financière Activité	Non	Non
Dossier médical	Gérer le dossier médical et de soins, les prescriptions Assurer la traçabilité des soins 15	Données d'identification Dossier médical, Prescription, relevés NIR, données sensibles	Non	Non
Support et Maintenance	Assurer la maintenance et l'Assistance auprès de nos Clients	Données d'identification collaborateur et /ou de résident	Atlassian Teamviewer	Non
NETContact	Gérer la fonction commerciale: admission et file d'attente	Données d'identification et de connexion	Non	Non
NETFactu	Gérer la facturation des résidents	Données d'identification résident, personne facturée Vie personnelle et financière, connexion	Non	Non
NETPlanning	Permettre la gestion du personnel de nos Clients	Données d'identification salarié, contrat de travail Connexion, NIR	Non	Non
NETPharmacie NETBiologie	Assurer le suivi médical des soins en lien avec les pharmacies et les laboratoires d'analyses	Données d'identification résident, dossier résident Vie personnelle NIR	Non	Non
NETDMP	Mettre les données médicales Résident à disposition des Médecins via la carte CPS	Données d'identification Connexion Dossier médical	Non	Non
NETTélémedecine	Maintenir le lien entre les résidents et les médecins via la téléconsultation	Données d'identification Connexion Dossier médical, prescription	Non	Non

Traitement	Finalité	Catégories Données	Sous-traitant	Transfert hors UE
NETFamille	Gérer les contacts des Résidents	Données d'identification Connexion	Non	Non
NETEntourage	Permettre l'accès partiel, au dossier résident, par les proches (habilités) des résidents	Données d'identification Activités, soins Résident Connexion	Non	Non

5.3. Liste des sous-traitants

Sous-traitant	Finalité	Localisation	Garanties
CLARANET	Hébergement HDS progiciels	France	Contrat Certifié HADS; ISO 27001
AWS	Hébergement des sauvegardes externalisées hors site	France	Contrat Certifié HADS; ISO 27001;...
AWS Cloudfront	WAF / CDN	UE	Contrat Certifié HADS; ISO 27001;...
TEAMVIEWER	Téléassistance, contrôle et accès à distance	UE	Contrat Certifié ISO 27001
ATLASSIAN (JIRA)	Support, conception et développement	UE	Contrat Certifié ISO 27001
MAILJET	Gestion des mails intégrés aux Solutions	UE	Contrat- CCT Certifié ISO 27001 - SOC2

Partenariat: le Prestataire intègre dans sa solution le module de prescription médicale sécurisée de la Banque Claude Bernard (RESIP). Bien que les données et fonctionnalités de la Banque Claude Bernard soient élaborées avec extrêmement de soins, le professionnel de santé est informé que du fait de la complexité du sujet, RESIP et le Prestataire déclinent toute responsabilité pour les conséquences éventuelles pouvant résulter d'une erreur de prescription, de délivrance ou d'utilisation de la Suite Logicielle.

[CGU- RESIP](#) - Base Claude Bernard

5.4. Mesures de sécurité encadrant la protection des données

Mesures	Description des mesures du Prestataire
Politique & Gouvernance	
PSSI	Le Prestataire dispose d'une PSSI formalisée et diffusée aux collaborateurs
Equipe Sécurité & Compliance	Le Prestataire dispose d'une équipe dédiée à la Sécurité et à la Compliance : Le RSSI travaille en étroite collaboration avec le DPO
Gestion des Risques	– Les risques sont identifiés, évalués et priorisés . Revue des risques à minima annuellement ou lors de changement ou incident notables
Gestion des Projets	L'équipe Sécurité & Compliance est associée aux projets pour évaluer la sécurité et les éventuels impacts sur les Données (Privacy by design)
Sécurité des applications	Réalisation régulière d'audit de codes, pour identifier les vulnérabilités potentielles, et de test de pénétration, par des tiers indépendants pour évaluer la résistance face aux attaques
Contrôle à l'embauche	Les équipes RH réalisent des vérifications avant l'embauche en accord avec la réglementation et le poste à attribuer. Un important dispositif de cooptation et de mobilité interne est déployé afin d'accueillir et de conserver des talents connus et reconnus.
Sensibilisation	Tous les employés reçoivent une formation régulière sur les obligations du RGPD et les bonnes pratiques en matière de sécurité des données. Des programmes de sensibilisation sont mis en place pour renforcer la culture de la protection des données au sein de l'entreprise.
Confidentialité	Les clauses de confidentialité sont intégrées au contrat de travail sur tous nos collaborateurs et aux contrats avec nos sous-traitants s'ils accèdent aux données. Les devoirs de confidentialité perdurent après la fin du contrat de travail ou de la prestation de service.
Gestion des Tiers	Les sous-traitants sont sélectionnés avec rigueur L'évaluation des sous-traitants critiques est réalisée régulièrement Les contrats encadrent la confidentialité, la sécurité et le RGPD si besoin
Sécurité logique et physique	
Gestion des Droits et Habilitations	Les habilitations sont gérées via des processus de gestion des accès, en fonction des besoins d'accéder via des profils définis. Les comptes sont nominatifs. Une revue des comptes d'accès est réalisée dès que besoin
Journalisation	Les traces des accès par les utilisateurs sont encadrées par la politique de journalisation. Les utilisateurs bénéficient d'un identifiant unique et nominatif garantissant l'imputabilité. Les accès de nos collaborateurs aux BDD sont tracés
Cloisonnement des données	Environnement de production séparé de l'environnement de sauvegarde. Les environnements Clients sont séparés de manière logique.
Chiffrement des données	En transit : Toutes les communications externes et internes sont chiffrées à l'aide de protocoles sécurisés tels que HTTPS avec SSL/TLS, assurant la sécurité des échanges entre les utilisateurs et nos applications.

Mesures	Description des mesures du Prestataire
	<p>Au repos : Les données stockées sur nos serveurs sont chiffrées à l'aide de l'algorithme AES avec une clé de chiffrement d'au moins 256 bits. Les sauvegardes sont également chiffrées pour garantir la confidentialité</p> <p>Gestion sécurisée des clés de chiffrement conforme aux meilleures pratiques</p>
Échanges & flux de données	<p>Sécurisation des communications : Les connexions distantes sont sécurisées via des réseaux privés virtuels (VPN) utilisant des protocoles robustes</p> <p>Tous nos flux de communication sont sur du TLS 1.2 à minima.</p> <p>Les échanges entre nos Clients/ partenaires et CIM sont tous sécurisés via PESIT-SSL 2-way, SFTP ou CF, VPN IPSEC</p>
Sécurisation des postes	Les postes de travail sont mis à jour, équipés d'un antivirus et de plusieurs mécanismes de protection
Support amovible	L'utilisation des supports amovibles est restreinte au strict nécessaire-uniquement en cas de besoin
Mise au rebut des supports	La mise au rebut des postes de travail : Si le poste est fonctionnel, celui-ci est formaté, le chiffrement préalable du disque garantit que les données ne pourront pas être récupérées après formatage. Dans le cas contraire, le disque dur est détruit.
Authentification	<p>Les informations secrètes d'authentification sont remises à l'utilisateur à l'initialisation de son compte, le secret est ensuite modifié par l'utilisateur et seulement connu de celui-ci.</p> <p>Les accès aux systèmes internes du Prestataire sont protégés par une authentification multifacteur (MFA)</p> <p>la complexité des mots de passe varie en fonction de la typologie du compte (utilisateur, admin, ...) et est conforme aux exigences de la CNIL et de l'ANSSI</p>
Accès aux locaux	Les accès aux centres de données sont protégés par des systèmes de contrôles d'accès – seul le personnel autorisé peut accéder aux zones sensibles conformément aux procédures d'accès strictes.
Environnements distincts	Une séparation des environnements pour permettre des développements et des tests hors production.
Sauvegardes	<p>Les prestations de sauvegardes incluent des tests de restauration annuels, ainsi que la fréquence quotidienne sur des supports sécurisés avec des copies externalisées.</p> <p>Avec une rétention sur 12 mois</p>

6. Label & Certification

Le Prestataire est certifiée ISO 13485. Cette certification garantit que le prestataire est engagé dans une démarche d'amélioration continue pour répondre aux exigences réglementaires et aux exigences Clients.

L'ensemble de nos certificats produits est disponible sur notre [site internet](#).