

Annexe Intellio Éditeurs

Version 1.3 – Février 2026

Préambule

Cette annexe "Solution" vient compléter les informations présentes dans les [CGV](#) d'Orisha Healthcare et accessibles sur notre site internet à l'adresse suivante <https://healthcare.orisha.com>.

Elle vient préciser les conditions et les traitements en lien avec la Solution Intellio Éditeurs souscrite et s'applique de plein droit.

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](#) accessibles sur notre site.

1.1. Redevance Proiciel récurrente

Les conditions financières sont négociées sur la base d'un engagement de 12 mois, mais elles peuvent être négociées sur la base d'un engagement ferme "Période initiale" de 2, 3 ou 4 ans précisé à la Proposition Commerciale.

Il est précisé que les factures récurrentes sont datées du premier jour ouvré de la période :

- En cas de Mise à Disposition entre le 1er et le 24 du mois M, la redevance est facturée à compter du premier jour du mois M,
- En cas de Mise à Disposition entre le 25 et le 31 du mois M, la redevance est facturée à compter du premier jour du mois M+1.

Au delà de l'éventuelle Période Initiale, les contrats sont renouvelés tacitement et annuellement sauf résiliation adressée 3 mois avant la date anniversaire en LRAR et le contrat prend fin le dernier jour du mois de fin de préavis.

La date anniversaire du contrat est basée sur la date de la première facturation de l'abonnement.

Toute résiliation du Contrat par le Client avant la fin de la Période Initiale, pour une raison non imputable à la société Orisha Healthcare France, donnera lieu à une

facturation de 50% du montant de la redevance restant à facturer jusqu'au terme de la Période Initiale.

Toute résiliation intervenant en cours d'année sera facturée des échéances dues jusqu'à la date anniversaire.

1.2. Prestation de formation

A la demande du Client, le Prestataire fournira une prestation de formation certifiée par Qualiopi, sur ses logiciels, applications informatiques vendus au Client dont le coût fera l'objet d'un détail sur la proposition commerciale qui sera soumise au Client.

2. Condition d'accès ou pré requis

Afin que Intellio Éditeurs soit utilisé dans les meilleures conditions il est impératif d'avoir une ligne SDSL avec un débit minimum de 0,2 Mbits/s/utilisateur. Soit 2 Mbits pour 10 utilisateurs. Ce prérequis est à appliquer par centre.

Les frais de mise en œuvre et de location étant intégralement à la charge du Client.

Configuration conseillée :

Version : Windows 10

Mémoire : 6 Go

Processeur : Intel Core i5 2.5GHz Hexa Core (9ème génération) ou équivalent

Résolution écran : $\geq 1920 \times 1080$

Navigateur : Google Chrome (V90+)

Configuration minimale :

Version : Windows 10

Mémoire : 4 Go

Processeur : Intel Core i5 2.3GHz Quad Core (6ème génération) ou équivalent

Résolution écran : $\geq 1920 \times 1080$

Navigateur : Google Chrome (V90+)

Recommandation

Pour la sécurité de vos données et pour la compatibilité de Intellio Éditeurs, les mises à jour Windows (Windows Update) doivent être réalisées régulièrement.

Compatibilité

	Poste avec lecteur de carte Vitale et/ou logiciel externe	Autre poste
Navigateur		
Firefox (V90+)	x	
Chrome (V90+)	x	
Architecture		
Framework.net (3.5)	x	

Mobilité

Pour une expérience mobile avec Intellio Éditeurs nous recommandons :

- Une tablette Microsoft Surface Pro 7 minimum avec la configuration suivante :
 - o Intel Core i5
 - o 8 Go de RAM
 - o 128 Go de stockage
- Un lecteur PC/SC bi-fente SENSYL DSC-FX

Une connexion 4G ou Wifi est nécessaire pour l'utilisation de Intellio Éditeurs et de ses services.

Ces prérequis sont susceptibles d'évoluer à chaque nouvelle version du progiciel. Les prérequis disponibles depuis [le site support Client](#) prévalent sur tout autre document.

3. Hébergement & infogérance

La présente description est donnée à titre indicatif par la société Orisha Healthcare France qui pourra faire évoluer le datacenter en fonction de ses besoins et des progrès de la technique, sans que cela nécessite la régularisation d'un avenant.

Les seuls engagements de la société Orisha Healthcare France sont, d'une part, de ne pas dégrader le niveau technique du datacenter et, d'autre part, la fourniture de ses prestations au titre de l'hébergement et de l'infogérance conformément aux Indicateurs Qualité convenus.

Notre offre s'appuie sur un hébergeur agréé Hébergement de Données de Santé, dont la certification est précisée à l'article 7.

Lorsque le Client importe et/ou stocke des Données dans le Progiciel, le Client accorde au Prestataire, ainsi qu'à ses sous-traitants, une licence, pour la France, d'hébergement, de stockage, de reproduction desdites Données uniquement en vue de l'exécution des Services. Cette autorisation demeure pour toute la durée du Contrat.

OFFRE DE SERVICES HÉBERGEMENT PROGICIELS DU PRESTATAIRE	PREMIUM
INFOGÉRANCE SERVEURS APPLICATIFS	Infogérance 5j/7 - heures ouvrées
INFOGÉRANCE CLUSTER BASE DONNEES	oui
SUPERVISION RÉSEAU DATACENTER + ACCÈS INTERNET ENTRANT	inclus
SAUVEGARDE	inclus
VOLUMÉTRIE DE STOCKAGE INCLUS OFFRE BASE	500 Go
PRA	OUI
RPO	15 minutes
RTO	4H
AGENT SUPERVISION PERFORMANCE	INCLUS
SLA : TAUX DE DISPONIBILITÉ	99,9 %

3.1 Plan de reprise d'activité (PRA) mis en place pour le service PREMIUM.

Cela signifie que les moyens techniques et organisationnels sont mis en œuvre avec pour mission d'assurer une très haute disponibilité répartie sur deux sites d'hébergement et qu'un incident majeur sur l'un des sites n'aura pas d'impact fonctionnel sur le service rendu et la disponibilité de la donnée de santé en respect des accords fixés entre les parties.

Une prise d'engagement sur cette continuité sera appuyée sur les garanties fournies par Le Prestataire et sur les mécanismes de réplication certifiés par ses soins (garantie d'intégrité et de confidentialité sur les données)

Sur chaque site d'hébergement seront déployés un nombre de serveurs équivalent ou presque, une ou plusieurs baies de disques selon les volumétries en

jeu ainsi que des clusters de Firewalls qui communiquent à travers d'un lien sécurisé.

L'ensemble des données et disques des machines virtuelles sont stockés sur les baies de disques exclusivement. Si les flux provenant de l'extérieur via un lien dédié sont à intégrer au PRA, un lien supplémentaire analogue à ceux mis en place sur site principal sera à déployer sur site secondaire.

Les serveurs sont tous redondés par réplication de sources applicatives et les bases de données sont répliquées avec des mécanismes synchrones ou mises en cluster. La répartition de charge entre les N serveurs frontaux se fait indépendamment des sites d'hébergement.

L'activation de ces mécanismes est nativement possible si tous les serveurs hôtes ont accès au réseau de stockage. Si le PRA doit comporter une activation de l'ensemble de ces mécanismes afin d'assurer une disponibilité maximale, le réseau de stockage devra s'étendre d'un datacenter à l'autre. La mise en œuvre d'un lien redondé dédié spécifique est donc à prévoir avec des équipements optimisés répondant aux exigences des équipements retenus.

3.2 SLA proposés dans le service PREMIUM

Dans le cas d'un PRA Infrastructure (Plan de Reprise en cas de sinistre majeur : panne matérielle, technologique, catastrophe naturelle, ...)

- Le RPO (Recovery Point Objectif), correspond à la perte de données maximales en cas de sinistre. Dans le cas d'un PRA, aucune perte de données n'est prévue

En effet les clusters PostgreSQL répartis sur les 2 Datacenter assurent l'acquittement des données sur les zones de stockage présentes sur les 2 sites.

- Le RTO (Recovery Time Objectif), correspond au temps de reprise en cas de sinistre. Dans le cas d'un PRA, aucune interruption de services liés à une défaillance matérielle n'est prévue. Il peut cependant y avoir une dégradation de la performance d'accès aux services du fait de l'indisponibilité des ressources informatiques qui sont impactées.

Tous les éléments de notre prestataire hébergeur et dédiés à la plateforme du Prestataire étant redondés et répartis sur les 2 sites, la continuité des services est assurée.

D'un point de vue SLA, nous garantissons une disponibilité des services d'infrastructures à hauteur de 99,9%. En cas d'incident sur un composant logiciel bloquant, nous garantissons une intervention (GTI) en moins de 1 Heure et un rétablissement (GTR) en moins de 4H.

3.3 Supervision & sécurité

Le Prestataire s'engage à respecter la Charte Qualité et notamment les points suivants qui sont le gage de la qualité de sa prestation, à savoir :

DISPONIBILITÉ – Disponibilité du service

Le Service est accessible du lundi au samedi de 8H00 à 20H00 (hors jour férié) (hors période de maintenance, planifiée ou non, de l'Environnement)

Par ailleurs, du lundi au samedi (hors jour férié) et de 8H00 à 20H00, Le Prestataire garantit sur cette plage un taux de disponibilité supérieur ou égal à 99,5 %

Le Prestataire garantit un temps de rétablissement du Service (pour la partie dont la responsabilité lui incombe) en 4 heures, le cas échéant en mode dégradé

Le PRA est natif dans l'abonnement.

Supervision de serveurs

Surveillance de la plateforme applicative et de la base de données hébergée:

Inspection physique journalière des équipements et des raccordements (température, installation physique, contrôle d'accès, alimentation et consommation électrique, afficheurs des systèmes, voyants, connections,)

Vérification de la disponibilité des serveurs, de la plateforme applicative et de la base de données

Gestion de la sauvegarde

Réalisation des sauvegardes journalières, mensuelles ou annuelles

Stockage des média de sauvegarde sur un site distant des sauvegardes hebdomadaires en toute sécurité,

Sauvegarde, archivage ou restaurations à la demande,

Test de restauration deux fois par an pour vérifier la conformité des médias et lecteurs

Conservation des médias de sauvegarde sur une année

Firewalling

Filtrage des ports

Surveillance des tentatives d'intrusion intempestive

SÉCURITÉ ET CONFIDENTIALITÉ

Le Prestataire a mis en place des contrôles efficaces de protection contre l'accès physique non autorisé aux systèmes d'exploitation et aux applications du Prestataire, 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.

La sécurité Internet est assurée par un cluster de firewalls, assurant une redondance des équipements et une haute disponibilité

La sécurité et la disponibilité des serveurs est assurée par la mise en place d'une solution de virtualisation.

La sauvegarde est assurée par une solution de dernière génération.

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

L'intégrité du traitement s'étend à toute composante du système et à toutes les phases du traitement (entrée de données, transmission, traitement, stockage et sortie des données). Ces contrôles consistent en des contrôles de cohérence des traitements, la détection et la gestion des anomalies ainsi que l'information des Utilisateurs nommés relativement à tout risque de non-conformité associée.

4. Création Portail Client

Chaque utilisateur Intellio Éditeurs aura accès à un espace Client en ligne.

La création de ce compte est gratuite et se fait lors de sa souscription aux solutions Intellio. A réception du mail de validation et d'activation de son espace, il devra avant la première connexion modifier son mot de passe personnel. L'utilisateur doit fournir des informations exactes et à jour, et s'engage à mettre à jour ces informations en cas de changement afin de continuer de bénéficier de l'accès.

Confidentialité : L'utilisateur est responsable de la confidentialité de ses identifiants de connexion qu'il définit lui-même et dont lui seul a connaissance.

Il s'engage à ne pas divulguer ces informations à des tiers. En cas de suspicion d'une utilisation non autorisée de son compte, l'utilisateur doit immédiatement en informer l'entreprise.

Utilisation du Compte : L'utilisateur s'engage à utiliser son compte d'une manière qui respecte les lois et réglementations en vigueur, ainsi que les CGV et la présente Annexe Solution. L'entreprise se réserve le droit de suspendre ou de fermer le compte en cas de non-respect de ces conditions.

L'utilisateur s'engage à mettre à jour et transmettre à Orisha toute modification relative à ses données administratives.

Services Disponibles : Une fois le compte activé, l'utilisateur pourra accéder à divers services en ligne 24/7, tels que :

- L'accès à ses factures d'abonnements et de prestations diverses.
- La gestion et le suivi des demandes de support, des réclamations.
- L'accès à la base de connaissance.
- La mise à jour des informations personnelles.

Modification des Services : Orisha Healthcare se réserve le droit de modifier, à tout moment, les services disponibles sur le portail Client et d'en informer les utilisateurs via le moyen de communication de son choix.

Fermeture du portail Client : l'accès au portail est désactivé 1 mois après la date de fin de contrat du Client.

5. Maintenance Progicielle et Support

La Documentation associée à la solution Intellio Éditeurs est mise à disposition du Client par Orisha Healthcare France depuis [le site support Client](#). Il appartient aux utilisateurs de se reporter à cette Documentation avant chaque demande.

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

La maintenance porte uniquement sur les progiciels et matériel souscrits auprès de Orisha Healthcare France.

5.1. Maintenance Progicielle corrective

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 par téléphone, portail web sous forme de ticket ou chatlive avec une précision suffisante pour que cette dernière puisse intervenir.

5.2. Maintenance Progicielle évolutive

Des mises à jour du Progiciel pourront être installées par le Prestataire sur son Environnement, au fur et à mesure de leur disponibilité. Ces mises à jour, qui sont décidées unilatéralement par Le Prestataire, seront mises à disposition du Client depuis son Environnement sans coût supplémentaire, dès lors qu'elles porteront sur des évolutions mineures. La fourniture de mises à jour intégrant des fonctionnalités et/ou des modules nouveaux par rapport à la dernière version majeure du Progiciel fera quant à elle l'objet d'un complément de redevance de licence.

5.3. Maintenance Progicielle réglementaire

Les différentes mises à jour auront pour objet de procéder à l'ensemble des modifications rendues nécessaires par les évolutions légales ou réglementaires correspondant aux traitements relatifs à la mise en œuvre du Progiciel.

Exclusions

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

- refus de la part du Client d'accepter une mise à jour ;
- 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. A 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 (voir Pré-requis).
- Modification, révision, changement ou entretien du Progiciel par d'autres personnes que les préposés de Le 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.

5.4. Cadre de la maintenance Support Client

Le Support Client est disponible du lundi au vendredi de 09h30 à 12h30 - 13h30 à 17h30.

Le Support Client n'est accessible qu'au Client ou l'utilisateur dénommé au contrat et que pour les logiciels commercialisés par Orisha Healthcare France, ce qui exclut les mises à niveau du système d'exploitation non effectuées par Orisha Healthcare France.

SERVICES MAINTENANCE PROGICIELS	GOLD
Forfait / Mois / ETP (équivalent temps plein) = 2 utilisateurs nommés	Petites et moyennes organisations
Accès support Clients niveau 1 (email, téléphone, chat)	
Accès support Clients niveau 2	x
Accès à la base de connaissance	x

SERVICES MAINTENANCE PROGICIELS	GOLD
2 utilisateurs nommés pour accéder au support en ligne	x
Prise en compte immédiate d'un ticket qualifié	x
Délai de réponse pour apporter une solution	48h ouvrées
Temps de clôture de la demande	96h ouvrées
Installation initiale et automatique des nouvelles versions	x
Installation nouvelles version soir et week-end	x
Installation du lecteur de carte	x
Monitorat et accompagnement	1h /mois
Audit Tiers Payant	
Audit métier	
Support Client niveau 1	
<p>Traitement des tickets n'impliquant pas un travail d'analyse long et un suivi moyen terme (Gestion des incidents). Traitement en temps réel des demandes pouvant être clôturées dans un délai maximum de 20 minutes.</p>	
Support Client niveau 2 et 3	
<p>Traitement des tickets complexes ou nécessitant un suivi régulier. Lien avec le service Développement pour les tickets nécessitant de rentrer dans la roadmap de version (gestion des problèmes). Traitement des tickets complexes nécessitant une expertise métier pointue, une intervention si nécessaire en base de données et l'assistance d'un collaborateur de l'équipe de développement.</p>	

A LA CHARGE de Orisha Healthcare France

Orisha Healthcare France, d'ores et déjà autorisée en cela par le Client, interviendra de sa propre initiative sur les logiciels, sans avertissement préalable, soit en raison de la détection d'une anomalie, soit en cas de modification de l'environnement légal, réglementaire ou médical.

Orisha Healthcare France apportera un support logiciel concernant les applicatifs développés par la Société. Le Service Support apportera aux utilisateurs les services suivants :

- Toutes les demandes seront tracées dans le CRM Orisha Healthcare France permettant d'analyser l'activité et rentrer dans un processus d'amélioration continue ;
- Le Client sera tenu d'accepter toute modification de logiciel proposée par Orisha Healthcare France, sachant que seule la dernière version sera maintenue. Les évolutions proposées dans les nouvelles versions pourront faire l'objet d'une facturation supplémentaire ;
 - Dans l'hypothèse où le service Support n'aurait pas permis d'aboutir à la correction de l'anomalie, Orisha Healthcare France pourra proposer une mise à jour des logiciels visés, ou une migration vers un produit répondant à ses besoins.
 - Une proposition de solution de contournement en cas d'anomalies
 - Une remontée au service développement en cas d'anomalie
 - Un renvoi vers les référents métier du Client si la demande est hors du périmètre Orisha Healthcare France

A LA CHARGE DU CLIENT

- Les problèmes liés à son infrastructure informatique, à son poste du travail (windows, autres), à son réseau (Wifi, internet, antivirus, firewall,...), ses périphériques (imprimante, scanner, douchette,) et aux applications externes au prestataire ;
- Maintenir un matériel non obsolète et permettant les mises à jour : le prestataire ne pourra être tenu responsable en cas d'impossibilité de mises à jour due à l'obsolescence du matériel du Client ;
- Installation des postes Clients
- La gestion du paramétrage des applications d'Orisha Healthcare France ;
- La consultation de la documentation des logiciels avant chaque appel téléphonique afin de décrire de façon précise et exhaustive les symptômes du dysfonctionnement rencontrés ;
- Les interventions rendues nécessaires par suite d'erreur de manipulation, d'absence de sauvegarde, de coupure de courant ou de panne matérielle seront facturées, selon devis préalable accepté par le Client ;
- La gestion des métiers et des cas d'utilisation liés au contexte du Client ;
- Le suivi financier de l'activité ;
- La formation des utilisateurs ;
- Les extractions des données spécifiques non présentes dans les applications.

Le Client demeure seul responsable de la **sécurisation de son poste de travail utilisateur**. Il lui incombe de mettre en œuvre toutes les mesures techniques nécessaires (mises à jour logicielles, antivirus, pare-feu) pour prévenir toute intrusion ou faille de sécurité. Le Prestataire décline toute responsabilité pour tout préjudice découlant d'un manquement du Client à ses **obligations de vigilance et de maintenance** informatique.

6. DESCRIPTION DES TRAITEMENTS DE DONNÉES

6.1. Traitements réalisés par Orisha Healthcare

Dans le cadre de la relation commerciale et contractuelle, Orisha Healthcare France 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 et échanges	Participant au projet, Direction, Administratif ...	Identité, coordonnées de contact	Google Drive Messagerie	Compte nominatif sécurisé par authentification Boîte mail sécurisée
Contrat et commandes	Direction, Administratif, Projet, Commercial	Identité, coordonnées de contact	Google Drive Messagerie Universign Salesforce	Accès par compte nominatif sécurisé par authentification Boîte mail sécurisée Chiffrement
Comptabilité	Administratif Direction Commercial	Identité adresse mail	SAGE CashOnTime	Accès par compte nominatif sécurisé par authentification
Newsletter et actualités	Participant au contrat ou au projet	Identité adresse mail	Mailjet Pardot Salesforce	Accès par compte nominatif sécurisé par authentification Clauses contractuelles type 2021 Chiffrement des données
Accès au site	Visiteur	Identité	N/A	conservation 1 an

Le Client est informé et accepte expressément que, conformément aux dispositions légales applicables :

- Le Logiciel comporte des dispositifs techniques qui, lors d'une connexion Internet, permettent au Client via un web service, soit automatiquement, soit le cas échéant à l'initiative de la Société, d'envoyer à la Société des informations sur l'identification du Client (adresse IP, jeton d'authentification...)

- Les cookies ont pour finalité exclusive de permettre ou faciliter la communication par voie électronique et sont strictement nécessaires à l'exécution du Contrat selon la demande expresse du Client. Les cookies sont de plusieurs types, en particulier :
 - Identifiant unique de session
 - Identification de serveur
 - Sécurité
 - Faciliter la navigation

Les informations obtenues par la Société grâce à ces dispositifs techniques sont également susceptibles d'être utilisées par la Société dans le cadre de la lutte anti-contrefaçon, pour repérer et empêcher une éventuelle utilisation illicite ou non-conforme du Logiciel.

6.2. Liste des traitements Intellio Éditeurs

Traitements de base Intellio Éditeurs sur instructions du Client

Objet	Finalité	Catégories Données	Sous - traitant	Transfert hors UE
Facturation	Moteur de facturation Sesam Vitale des FSE: FSE, lot ... Boîte aux lettres Sesam Vitale	Norme GIE Sesam Vitale	Non	Non
ADRI	Interrogation via API de la plateforme de l'assurance Maladie sur les droits des patients et niveau de couverture	Identité, NIR, date de naissance, code régime du patient Niveau de couverture	Non	Non
DPEC	Demande de Prise en Charge électronique : Interrogation via API de la prise en charge par la mutuelle du patient	Norme GIE Sesam Vitale Archivage des échanges AMC- PS	Non	Non
GED	Gestion documentaire PS : Enregistrement et indexation des documents par les PS	Tout document susceptible d'être déposé par le PS	Non	Non
Hébergement	Hébergement HADS BDD, copies, sauvegardes pour assurer la continuité d'activité et les tests	Données présentes en BDD	CHEOPS AWS CLARANET	Non
Support et Maintenance	Support Client selon le niveau souscrit par le Client Ticketing sur anomalies ou maintenance	Identité collaborateur Client Potentielles données patient si besoin	Salesforce	Non

Les téléservices pour lesquels nous avons l'agrément sont décrits sur notre site et mis à jour régulièrement.

6.3. Mesures de sécurité

Le Groupe Orisha met en place une protection des données renforcée au travers de mesures organisationnelles et techniques appropriées pour préserver la sécurité, l'intégrité et la confidentialité de vos données.

Mesures	Description des mesures
Mesures Techniques	
Tracer les accès	Journalisation des interventions Traçabilité de l'ensemble des exports réalisés sur l'outil
Protéger le réseau informatique	Limitation des flux réseau au strict nécessaire Protocole d'échange avec les concentrateurs CFT et double SSL
Sécuriser les serveurs	Limitation des accès aux outils et interfaces d'administration aux seules personnes habilitées Installation sans délai des mises à jour critiques Assurer la disponibilité des données
Sécuriser les sites web	Protocole SSL Aucun mot de passe ou identifiant dans les Urls Contrôler que les entrées des utilisateurs correspondent à l'attendu
Continuité d'activité	Sauvegardes automatiques selon le plan de sauvegarde défini
Sécuriser les échanges	Chiffrement des données lors des échanges entre Organismes
Protéger les locaux	Sécuriser les accès par des portes verrouillées Installer des alarmes anti-intrusion et les vérifier régulièrement
Cryptographie	Utiliser des algorithmes, des logiciels et des bibliothèques reconnus Conserver les secrets et les clés cryptographiques de manière sécurisée
Mesures de Gouvernance	
Gérer les habilitations	Définition des profils d'habilitation Suppression des permissions d'accès obsolètes Revue régulière des habilitations
Encadrer la maintenance et la destruction des données	Enregistrer les interventions de maintenance dans un main courante Effacer les données de tout matériel avant mise au rebut
Archiver en sécurité	Accès limité aux archives et sauvegardes Sécurisation des sauvegardes

Mesures	Description des mesures
Procédures	Procédure de notification de violation de données Procédure de gestion des habilitations
Sensibilisation des collaborateurs	Sensibilisation à la sécurité et à la protection des données Clause de confidentialité intégrée au contrat de travail Charte informatique contraignante PSSI formalisée et diffusée aux collaborateurs
Encadrer les développements	Proposer des paramètres respectueux de la vie privée aux utilisateurs finaux Une séparation des environnements pour permettre des développements et des tests hors production.

Mesures de la responsabilité du Client :

- Le Client détermine ses délais de conservation des données.
- Le Client est responsable de la gestion des habilitations de ses collaborateurs.
- Le Client est responsable de la sécurisation des flux qu'il adresse

6.4. Liste des sous traitants

Sous-traitant	Finalité	Lieu	Garanties
AWS	Cloud Provider hébergement infrastructure	France	Contrat Certifié HADS, ISO 27001 ... Data Privacy Framework
Cheops Technology	Datacenter - Hébergement infrastructure	France	Contrat Certifié HADS, ISO 27001 ...
Claranet	Infogéreur	France	Contrat Certifié HADS, ISO 27001
Salesforce	CRM et ticketing support et maintenance	France	Contrat Clauses Contractuelles Type Certifié HADS, ISO 27001
Mailjet	Mailing & newsletter B2B	Allemagne - Belgique	Contrat ISO 27001
Atlassian	Développement et ticketing R&D	Allemagne	Contrat Certifié ISO 27001

7. Label & Certification

Les labels et certifications sont disponibles ci-dessous :

Équipements et logiciels labellisés

CNDA (Centre National de Dépôt et d'Agrément):

[Logiciels certifiés | CNDA](#)

AWS

- **HDS:** [Liste des hébergeurs certifiés | Agence du Numérique en Santé](#)
- **AWS** dispose de certifications de conformité aux normes ISO/IEC [27001:2022](#), [27017:2015](#), [27018:2019](#), [27701:2019](#), [22301:2019](#), [20000-1:2018](#), [9001:2015](#) et [CSA STAR CCM v4.0](#)

<https://aws.amazon.com/compliance/iso-certified/>



CLARANET

- **HDS:** [Liste des hébergeurs certifiés | Agence du Numérique en Santé](#)
- **Certification ISO 27001:**



SALESFORCE

- **HDS** : [Liste des hébergeurs certifiés | Agence du Numérique en Santé](#)
- **Certification ISO 27001**



Orisha Health & Safety

10 rue du Docteur Lancereaux - 75008 Paris- France
SASU au capital de 2 287 400,12 €
SIREN 982 117 772

CHEOPS TECHNOLOGY FRANCE

- **HDS :** [Liste des hébergeurs certifiés | Agence du Numérique en Santé](#)
- **Certification ISO 27001**



Certificat

Certificate

N° 2018/80964.8

Page 1 / 1

AFNOR Certification certifie que le système de management mis en place par :
AFNOR Certification certifies that the management system implemented by:

CHEOPS TECHNOLOGY FRANCE

pour les activités suivantes :
for the following activities:

- HEBERGEUR D'INFRASTRUCTURE PHYSIQUE ET HEBERGEUR INFOGEREUR
1. LA MISE A DISPOSITION ET LE MAINTIEN EN CONDITION OPERATIONNELLE DES SITES PHYSIQUES PERMETTANT D'HEBERGER L'INFRASTRUCTURE MATERIELLE DU SYSTEME D'INFORMATION UTILISE POUR LE TRAITEMENT DES DONNEES DE SANTE
 2. LA MISE A DISPOSITION ET LE MAINTIEN EN CONDITION OPERATIONNELLE DE L'INFRASTRUCTURE MATERIELLE DU SYSTEME D'INFORMATION UTILISE POUR LE TRAITEMENT DE DONNEES DE SANTE
 3. LA MISE A DISPOSITION ET LE MAINTIEN EN CONDITION OPERATIONNELLE DE LA PLATEFORME D'HEBERGEMENT D'APPLICATIONS DU SYSTEME D'INFORMATION
 4. LA MISE A DISPOSITION ET LE MAINTIEN EN CONDITION OPERATIONNELLE DE L'INFRASTRUCTURE VIRTUELLE DU SYSTEME D'INFORMATION UTILISE POUR LE TRAITEMENT DES DONNEES DE SANTE
 5. L'ADMINISTRATION ET L'EXPLOITATION DU SYSTEME D'INFORMATION CONTENANT LES DONNEES DE SANTE
 6. LA SAUVEGARDE DE DONNEES DE SANTE
- DECLARATION D'APPLICABILITE Version 3.0

CHEOPS TECHNOLOGY FRANCE est certifié selon la NF EN ISO/IEC 27001:2022

a été évalué et jugé conforme aux exigences requises par :
has been assessed and found to meet the requirements of:

REFERENTIEL DE CERTIFICATION HDS 1.1 - Mai 2018

et est déployé sur les sites suivants :
and is developed on the following locations:

siège : 37 RUE THOMAS EDISON FR-33610 CANEJAN
agence : 3 ROUTE DE LYON FR-69530 BRIGNAIS
DATACENTER EQUINIX BX1 : 39 RUE DE STRASBOURG FR-33520 BRUGES
DATACENTER SFR : 1 RUE DU DOCTEUR GABRIEL PERI FR-33300 BORDEAUX

Ce certificat est valable à compter du (année/mois/jour)
This certificate is valid from (year/month/day)

2024-11-14

Jusqu'au
Until

2026-05-15

Ce document est signé électroniquement. Il constitue un original électronique à valeur probante.
This document is electronically signed. It stands for an electronic original with probative value.

Julien NIZRI
Directeur Général d'AFNOR Certification
Managing Director of AFNOR Certification



Flashez ce QR
Code pour vérifier la
validité du certificat

Seul le certificat électronique, accessible sur www.afnor.org, est la preuve de la certification. Le certificat papier n'est qu'une copie.
Only the electronic certificate, accessible on www.afnor.org, is the proof of certification. The paper certificate is only a copy.

11 rue François de Pressensé - 93571 La Plaine Saint-Denis Cedex - France - T. +33 (0)1 41 62 80 00 - F. +33 (0)1 49 17 90 00
SAS au capital de 18 187 000 € - 479 076 002 RCS Bédoulay - www.afnor.org

afnor
CERTIFICATION

ATLASSIAN (JIRA):

- [Certification ISO 27001](#)
- [DPA](#)

		CERTIFICATE NUMBER: 2021-111501	
<h1>CERTIFICATE OF REGISTRATION</h1> <h2>Information Security Management System – ISO/IEC 27001:2022</h2>			
Coalfire Certification, Inc. certifies that the following organization operates an Information Security Management System (ISMS) that conforms to the requirements of ISO/IEC 27001:2022 per the scope and boundaries statement detailed below:			
COMPANY:	Atlassian Corporation Plc	ADDRESS:	363 George Street Sydney, NSW 2000 Australia
Scope:			
<p>The certificate scope comprises the Information Security Management System (ISMS) also referred to as the Atlassian Trust Management System supporting the operations underlying the Atlassian Cloud offering. The cloud offering comprises of Atlas, Atlassian Admin (including Guard Standard), Atlassian Analytics, Bitbucket Cloud (including Bitbucket Pipelines), Compass, Confluence Cloud (including Whiteboards and Databases), Connect, Data Lake, Forge, Guard Premium, Jira Align, Jira (including Automation for Jira and Jira Work Management), Jira Product Discovery, Jira Service Management (including Assets, Data Manager, JSM Chat, JSM Operations), Loom, Rovo, Statuspage, Trello as well as the micro services used to deliver these applications. These activities are governed by the implemented controls in accordance with the organizational Statement of Applicability, which further extends to the additional controls defined within ISO/IEC 27018:2019. The organizational scope includes the Legal, Talent, Privacy, Procurement, Trust (Security and Risk & Compliance), Workplace Experience, Cloud Engineering, Product Engineering, and Workplace Technology teams affecting the ISMS.</p>			
STATEMENT OF APPLICABILITY: VERSION: 11 DATE: September 10, 2024 ON BEHALF OF COALFIRE CERTIFICATION, INC.			
Original Registration Date: January 23, 2019 Certificate Issuance Date: November 27, 2024 Expiration Date: January 21, 2028	 Booker Young, VP of Global Assurance  		
This certificate relates to the Information Security Management System, and not to the products or services of the certified organization. The certification reference number, the mark of the certification body and/or the accreditation mark may not be shown on products or stated in documents regarding products or services. Promotional material, advertisements or other documents showing or referring to this certificate, the trademark of the certification body, or the accreditation mark, must comply with the intention of the certificate.			