Annexe DDM

Version 1.2 - Janvier 2025

Préambule:

Cette annexe vient compléter les informations présentes dans les CGV d'Orisha Health & Safety accessibles sur le site internet à l'adresse suivante https://insurance.orisha.com.
Elle vient préciser les conditions et les traitements en lien avec la Solution DDM 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 récurrente

Les conditions financières sont négociées sur la base d'un engagement ferme "Période initiale" de 3 ans sauf autre accord précisé à la Proposition Commerciale.

La première facturation est datée du 1er jour ouvré de la période de mise à disposition de la Solution.
- 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.

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 au Prestaire, donnera lieu à une facturation de 50% du montant de la redevance restant à facturer jusqu'au terme de la Période Initiale.

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

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

1.2. Location maintenance évolutive

En contrepartie de la concession du droit d'utilisation des Progiciels décrits dans les Propositions Commerciales, de l'hébergement et de l'infogérance des solutions, le licencié paiera une redevance annuelle, facturée trimestriellement à échoir, selon la tarification convenue dans la Proposition Commerciale.
La maintenance locative est facturée en fonction du nombre de salariés traités par DDM, sauf disposition contraire précisée dans la Proposition Commerciale.

1.3. Transport et frais de vie

Les modalités seront convenues entre les Parties.
Les frais de vie et de transport seront facturés aux frais réels.

1.4. Tarif journalier des prestations

Les prestations non définies dans la Proposition Commerciale donneront lieu, le cas échéant, à l'application des tarifs et conditions de règlement 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 accessibles sur notre site.

1.5. Facturation en mode projet

Pour de nouveaux projets, la facturation à date de livraison en recette sera au minimum fixée à 90% du montant initial devisé. Les 10% restant seront facturés à réception du procès-verbal de recette définitif engageant la mise en production.
Les Parties peuvent convenir d'un autre échéancier de facturation sur la Proposition Commerciale signée. Sans précision d'un échéancier de facturation spécifique, l'échéancier préalablement cité s'appliquera.
Le Client dispose de 45 jours calendaires pour effectuer la recette, sauf dérogation écrite entre les Parties.
A l'issue du délai de 45 jours, la recette sera de facto « prononcée » et la facturation du montant restant dû du projet et du locatif associé (le cas échéant) seront engagés.

1.6. Prestation de formation

Le Prestataire conseille vivement la formation " Module Formation à la DSN".
La formation peut se faire en présentiel ou en distanciel, selon le choix du Client.

- Prérequis technique en distanciel:
  - 1 ordinateur par participant
  - 1 connexion internet
- Maximum de participants à la formation : 7 participants par groupe

Un règlement sera remis à chaque participant à la formation.
A ce jour, la société CIM est certifiée Qualiopi.

1.7. Modalités de réversibilité

La prestation de réversibilité fera l'objet d'une qualification et d'un chiffrage adapté au scénario retenu par les Parties, sauf disposition contractuelle contraire, et sera à régler à réception de la facture.

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.

2. Condition d'accès et prérequis

Afin que DDM soit utilisé dans les meilleures conditions, il est impératif d'avoir :

- Un navigateur internet à jour et supporté par l'éditeur
- Un accès internet

3. Hébergement et infogérance

Le Client a retenu Le Prestataire comme partenaire pour assurer l'infogérance et l'hébergement de la solution DDM.
La présente description est donnée à titre indicatif par Le Prestataire, 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 du Prestataire 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.

L'offre du Prestataire s'appuie sur un hébergeur agréé Hébergement de Données de Santé et ISO 27001.
Voir " Certifications & Labels"
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.

3.1. Périmètre

Le périmètre d'hébergement et d'infogérance est précisé dans la Proposition Commerciale selon les solutions souscrites.

3.2. Sauvegardes

Le Prestataire garantit au Client un plan de sauvegarde défini comme suit:

- Sauvegarde quotidienne sur 7 jours.
- Sauvegarde mensuelle glissante
- Sauvegarde annuelle conservée 3 ans

3.3. PCA / PRA

Toutes les composantes de l'infrastructure de l'hébergeur technique du Prestataire, dédiées à la plateforme, sont redondées et développées pour être résilientes au travers de 2 Instances situées en France ou Union Européenne, qui assurent la Continuité d'Activité (Multi Availability Zone).
Cela signifie que les moyens techniques et organisationnels sont mis en œuvre avec pour mission d'assurer une très haute disponibilité répartie sur deux instances et qu'un incident majeur sur l'une des instances n'aura pas d'impact fonctionnel sur le service rendu et la disponibilité de la donnée en respect des accords fixés entre les Parties.
Une prise d'engagement sur cette continuité sera appuyée sur les garanties fournies par l'hébergeur technique du Prestataire et sur les mécanismes de réplication certifiés par ses soins (garantie d'intégrité et de confidentialité sur les données)

4. Support et Maintenance

La Documentation associée aux Solutions est mise à disposition du Client par Le Prestataire.
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 le service support du Prestataire. 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.

4.1. Procédure Support

Les demandes sont adressées par mail à support-dsn@ORISHA.com. ou sur le portail de ticketing mis à disposition des Clients.

A partir des informations, Le Prestataire procède au diagnostic et le cas échéant à la correction des Anomalies en indiquant au Client par téléphone, par courriel ou par le biais du portail, la procédure à suivre.

Le Prestataire met à disposition du Client un portail afin de lui permettre de signaler tous problèmes rencontrés. Ce portail (également appelé outil de ticketing) est accessible 7 jours sur 7, 24 heures sur 24. Il constitue le point d'entrée à privilégier qui assure l'accueil, la notification, la prise en compte, l'aiguillage et le suivi des demandes du Client. Les tickets sont récupérés en temps réel par le Support aux horaires ouvrés.

Le Client s'engage à utiliser, en toutes hypothèses, cet outil de communication pour signaler les difficultés rencontrées, y compris pour confirmer d'éventuels signalements effectués par mail. Toute demande d'intervention réalisée sur ce portail reçoit un numéro d'identifiant unique. Ce numéro de référence sera nécessaire au suivi.

Le portail permet la réalisation des services suivants :

- Identifier l'utilisateur, vérifier son habilitation, identifier le Client et le Contrat
- Qualifier la nature de sa demande
- Classifier l'Anomalie selon son niveau de sévérité
- Transmettre la demande au service compétent
- Informer le Client de l'état d'avancement de la demande
- Assister le Client à distance
- Assurer le traitement de la demande et sa traçabilité jusqu'à sa clôture.

Toute remontée d'Anomalie qui ne suivrait pas ce canal obligatoire ne pourra être prise en compte pour l'appréciation des Indicateurs Qualité par la société Le Prestataire.

4.2. Délai d'intervention et suivi

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.
Les délais sont mentionnés en Heures / Jour Ouvrés.

Anomalie	Délai d'Intervention	Délai pour solution de contournement	Délai de Résolution d'Anomalie ou clôture du ticket
Bloquante	2 heures ouvrables	1 jour ouvrable	5 jours ouvrables
Majeure	4 heures ouvrables	2 jours ouvrables	10 jours ouvrables
Mineure			Version mineure suivante

4.3. Maintenance

Maintenance corrective

La prestation de maintenance corrective consiste en la correction de toute Anomalie reproductible ou avérée qui apparaît dans l'utilisation de l'accès distant du Progiciel.

Maintenance 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.

Maintenance 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 à la Maintenance

Le Prestataire n'assurera pas le service de maintenance dans les cas suivants :

- Utilisation non conforme à la documentation de l'accès distant ;
- 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 incompatible avec les Progiciels, objet des présentes.
- 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. 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 -Finalité	Personnes concernées	Catégories Données	Sous-traitant & logiciel	Sécurité & garanties
Projet & échanges	Participant au projet, Direction, Administratif …	Identité, coordonnées de contact	Google Workspace	Compte nominatif sécurisé par authentification Boîte mail sécurisée
Contrat et commandes	Direction, Administratif, Projet, Commercial	Identité, coordonnées de contact	Google Workspace	Compte nominatif sécurisé par authentification Boîte mail sécurisée Chiffrement
Comptabilité	Administratif Direction Commercial	Identité adresse mail	SAGE CashOnTime	Compte nominatif sécurisé par authentification
Newsletter & communication actualité	Participant au contrat ou au projet	Identité adresse mail	Salesforce	Compte nominatif sécurisé par authentification Clauses contractuelles type 2021 Chiffrement des données
Accès aux locaux	Visiteur	Identité	Non	Conservation 1 an Habilitation limitée

5.2. Traitements DDM sur instruction du Client

Traitement	Finalité	Catégories Données	Sous-traitant	Transfert hors UE
Comptes-rendus métiers DSN	Générer les Comptes-Rendus Métiers (CRM) Mettre à disposition les CRM auprès des Concentrateurs Valider la qualité et la bonne réception du flux	Norme NEODES		Non
Consolidation des flux DSN	Contrôler la conformité des données en lien avec la fiche de paramétrage Garantir l'intégrité Assurer la cohérence	Norme NEODES		Non
Exports	Exports standards -Formatés aux normes réglementaires	Norme NEODES		Non
Hébergement DSN	Mettre à disposition les informations nécessaires au fonctionnement des solutions pour nos Clients Hébergés	Norme NEODES	AWS	Non
Intégration des flux DSN	Intégrer les fichiers DSN Historiser les données DSN	Norme NEODES		Non
API DSN	Mise à disposition des données au travers de l'API pour les Clients Lecture- Export	Norme NEODES	AWS	Non
Support et Maintenance	Assurer la maintenance et l'Assistance auprès de nos Clients	Identité collaborateur Client et potentielles données adhérent si besoin	Salesforce JIRA	Non

5.3. Liste des sous-traitants

Sous-traitant	Finalité	Localisation	Garanties
AWS	Cloud Provider (sans accès aux données)	France UE	Contrat Certifié HADS; ISO 27001;...
SALESFORCE	Support - ticketing et maintenance	France	Contrat Clauses Contractuelles Type Certifié HADS, ISO 27001
ATLASSIAN (JIRA)	Développement - ticketing et maintenance	Allemagne	Contrat Certifié ISO 27001

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 la DPO
Gestion des Risques	Une gestion des risques est mise œuvre et revue à minima annuellement ou lors de changement ou incident notables conformément à la certification ISO 27001
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)
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. La vérification des casiers judiciaires peut être réalisée sur les postes à risque ou stratégiques.
Sensibilisation	L'ensemble des collaborateurs, et quand cela est pertinent, les sous-traitants bénéficient d'une sensibilisation avec évaluation et de formations adaptées à la sécurité et à la protection des données - incluant les règles applicables et les conséquences d'un incident, d'une violation, d'une non-conformité...
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.
Relation avec les Tiers	Les sous-traitants sont sélectionnés avec rigueur L'évaluation des sous-traitants critiques est mise à jour annuellement dans le cadre de la Certification ISO 27001. Les contrats encadrent la confidentialité, la sécurité et le RGPD si besoin.

Mesures	Description des mesures du Prestataire
	Sécurité logique et physique
Gestion des Droits et Habilitations	Les habilitations sont gérées en cohérence avec la politique de contrôle d'accès et le besoin d'accéder via des profils définis. Une revue des comptes d'accès est réalisée mensuellement .
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	Nos sauvegardes sont chiffrées via les protocoles de chiffrements Advanced Encryption Standard 256 bits (AES-256)
Echanges & flux de données	Tous nos flux de communication sont sur du TLS 1.2 à minima. Les échanges entre nos Clients/ partenaires et CIM sont tous sécurisés via PESIT-SSL 2-way, SFTP ou CF, VPN IPSEC
Poste chiffré	Les postes de travail sont chiffrés, 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	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. la complexité des mots de passe varie en fonction de la typologie du compte (utilisateur, admin, ...) et est conforme aux recommandations de la CNIL- complétée selon la situation, par un mécanisme d'authentification multifacteur
Accès aux locaux	L'accès au bâtiment est sécurisé par un badge nominatif. Les visiteurs doivent compléter le registre dédié et être accompagnés d'un collaborateur. Le bâtiment est équipé d'un système de vidéosurveillance et d'une alarme anti-intrusion Les accès en datacenter sont strictement encadrés, limités et tracés
Environnements distincts	Une séparation des environnements pour permettre des développements et des tests hors production.
Sauvegardes	Les prestations de sauvegarde prennent en compte les modalités de restauration et incluent, le cas échéant, les tests, ainsi que la fréquence des sauvegardes dans un plan de sauvegarde

6. SLA - Objectifs de service

Objet	Indicateur	Valeur
Taux de disponibilité de la Plateforme DDM		99% hors plages de maintenances programmées
Disponibilité du service	Respect des plages horaires	Jours ouvrés de 7h à 19h
	Respect du calendrier	Tous les jours ouvrés
Gestion de compte Administrateur Client	Réception de la demande durant les plages horaires et dans le respect du calendrier	12 h pour la Création 4 h pour réinitialisation ou déverrouillage
Disponibilité du support	Respect des plages horaires	9h00-12h30 et 14h-18h00 du lundi au jeudi 9h00-12h30 et 14h-17h00 le vendredi

7. Labels & Certifications

Orisha Healthcare - CIM:

- **Rapport ISAE 3402 de type 1** pour son système de contrôle interne. Réalisé par les auditeurs de la société Grant Thornton.
- **Certification ISO 27001**

Certificat

LABORATOIRE NATIONAL DE MÉTROLOGIE ET D'ESSAIS

Certificate of Registration

Numéro de certificat 38111-4
Certificate number

CONSEILS ET INFORMATIQUE DE LA METROPOLE

8 AVENUE DE L'HORIZON PARC SCIENTIFIQUE HAUT BORNE
FRANCE - 59650 - VILLENEUVE D'ASCQ

met en œuvre et entretient un Système de Management de la Sécurité de l'Information conforme aux exigences de la norme
operates an Information Security Management System which complies with the requirements of

ISO/IEC 27001 : 2022 / NF EN ISO/IEC 27001 : 2023

Pour les activités suivantes / for the activities detailed below

Hebergement, infogérance et mise à disposition de solutions logicielles pour les mutuelles et courtiers en assurance.

Hosting, outsourcing and provision of software solutions for mutuals and insurance brokers.

Déclaration d'applicabilité / Statement of applicability
ENR-0002- STATEMENT OF APPLICABILITY V1.7 du 25/07/2024
Site(s) concerné(s) / Concerned location(s)
voir addendum / see addendum

Date début de validité 20 décembre 2024
Effective date December 20th, 2024

Valable jusqu'au 08 février 2028
Expiry date February 8th, 2028

Renouvelle / Renews le certificat 38111-3

Pour le Directeur Général
For the General Director

LUC CHAUSSON ID

Signature numérique de LUC CHAUSSON ID

Responsable du Département Certification en Technologies de l'Information
Head of Information Technologies Certification Department

Ce certificat est délivré conformément aux règles générales de certification LNE des systèmes de management d'entreprise.
This certificate is granted under the LNE regulations for registration.

Laboratoire national de métrologie et d'essais - 1, rue Gaston Boissier – 75724 PARIS Cedex 15

AWS

- **HDS – Hébergeur certifié :**

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/

DocuSign Envelope ID: D2CCB630-5150-4C94-8C4C-C6C70F13AA90

MGMT. SYS. RvA C 466

Certificate

Certificate number: 2013-009

Certified by EY CertifyPoint since: November 18, 2010

Based on certification examination in conformity with defined requirements in ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015/A1:2020, the Information Security Management System as defined and implemented by

Amazon Web Services, Inc.*

and its affiliates (collectively referred to as Amazon Web Services (AWS)) are compliant with the requirements as stated in the standard:

ISO/IEC 27001:2022

Issue date of certificate: November 18, 2022
Re-issue date of certificate: November 22, 2023
Expiration date of certificate: October 31, 2025
Last certification cycle expiration date: November 30, 2022

EY CertifyPoint will, according to the certification agreement dated April 1, 2022, perform surveillance audits and acknowledge the certificate until the expiration date noted above.

*With regard to the specific requirements for information security as stated in the Statement of Applicability, version 2023.02 dated September 12, 2023, this certification is applicable to (a) the services and their associated assets and locations as described in the scoping section of this certificate, and (b) any affiliates that are responsible for, or that contribute to, the provision of such services and their associated assets and locations.

DocuSigned by:
Jatin Sehgal
3DADCF3CCF6943C...

J. Sehgal | Director, EY CertifyPoint

This certificate is not transferable and remains the property of Ernst & Young CertifyPoint B.V., located at Antonio Vivaldistraat 150, 1083 HP, Amsterdam, the Netherlands. Any dispute relating to this certificate shall be subject to Dutch law in the exclusive jurisdiction of the court in Rotterdam. The content must not be altered and any promotion by employing this certificate or certification body quality mark must adhere to the scope and nature of certification and to the conditions of contract. Given the nature and inherent limitations of sample-based certification assessments, this certificate is not meant to express any form of assurance on the performance of the organization being certified to the referred ISO standard. The certificate does not grant immunity from any legal/ regulatory obligations. All rights reserved. © Copyright

Page 1 of 7 Digital version

SALESFORCE

- **HDS :** Liste des hébergeurs certifiés | Agence du Numérique en Santé
- **Certification ISO 27001**

Docusign Envelope ID: B78377E3-E451-4950-9906-F90E81A34992

MGMT. SYS. RvA C 466

Certificate

Certificate number: 2021-004

Certified by EY CertifyPoint since: January 28, 2021

Based on certification examination in conformity with defined requirements in ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015/A1:2020, the Information Security Management System as defined and implemented by

Salesforce, Inc.*

located in San Francisco, California, United States of America is compliant with the requirements as stated in the standard:

ISO/IEC 27001:2022

Issue date of certificate: January 25, 2024
Re-issue date of certificate: December 19, 2024
Expiration date of certificate: January 27, 2027
Last certification cycle expiration date: January 27, 2024

EY CertifyPoint will, according to the certification agreement dated April 30, 2024, perform surveillance audits and acknowledge the certificate until the expiration date noted above.

**The certification is applicable for the assets, services and locations as described in the scoping section at the back of this certificate, with regard to the specific requirements for information security as stated in the Statement of Applicability, version 4, dated November 27, 2024.*

DocuSigned by:
Jatin Sehgal
3DADCF3CCF6943C...

J. Sehgal | Director, EY CertifyPoint

This certificate is not transferable and remains the property of Ernst & Young CertifyPoint B.V., located at Antonio Vivaldistraat 150, 1083 HP, Amsterdam, the Netherlands. Any dispute relating to this certificate shall be subject to Dutch law in the exclusive jurisdiction of the court in Rotterdam. The content must not be altered and any promotion by employing this certificate or certification body quality mark must adhere to the scope and nature of certification and to the conditions of contract. Given the nature and inherent limitations of sample-based certification assessments, this certificate is not meant to express any form of assurance on the performance of the organization being certified to the referred ISO standard. The certificate does not grant immunity from any legal/ regulatory obligations. All rights reserved. © Copyright

ATLASSIAN (JIRA) :

- Certification ISO 27001
- DPA

ORISHA Insurance | Cim

DSNDataManager

COALFIRE CERT

CERTIFICATE NUMBER:
2021-111501

CERTIFICATE OF REGISTRATION

Information Security Management System – ISO/IEC 27001:2022

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:

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.

STATEMENT OF APPLICABILITY:
VERSION: 11
DATE: September 10, 2024

Original Registration Date:
January 23, 2019

Certificate Issuance Date:
November 27, 2024

Expiration Date:
January 21, 2028

ON BEHALF OF COALFIRE CERTIFICATION, INC.

Booker Young, VP of Global Assurance

COALFIRE ISO 27001 CERTIFIED CERT

ANAB ACCREDITED MANAGEMENT SYSTEMS CERTIFICATION BODY

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.