Plan d'Assurance Sécurité

ARONE

novembre 21

Date de validation :	JJ/MM/YYYY
Version :	0.91
Liste de diffusion :	Restreinte
Etat du document :	Interne

2 imp. Joséphine Baker
44800 Saint-Herblain
FRANCE

www.ot-group.com
Tel : +33.2.28.03.78.78

TABLE DES MATIÈRES

SECTION 1 - OBJECTIF DU PLAN D'ASSURANCE SÉCURITÉ

Le Plan d'Assurance Sécurité est une pièce portée en annexe du contrat qui lie le prestataire d'hébergement et de services managés [PRESTATAIRE], dénommé ci-après le « prestataire » et d'autre part la société [CLIENT] qui confie au prestataire son architecture applicative dénommé ci-après le « client ».

La structure du document s'inspire fortement du « Guide d'externalisation des systèmes d'information » édité par l'ANSSI. Cette dernière est communément reprise dans les appels d'offres publics et privés. L'évaluation et la pertinence de la couverture des exigences de sécurité sont ainsi simplifiées.

Le Plan d'Assurance Sécurité (PAS) décrit les dispositions de sécurité particulières mises en œuvre sur le projet, réputées satisfaire les exigences des partenaires du projet en matière de sécurité, définie en accord avec le client.

Ce PAS définit les méthodes, l'organisation et les activités d'assurance sécurité spécifiques au projet d'hébergement des services du client sur la plateforme mis en œuvre par le prestataire.

Ces objectifs sont les suivants :

- Constituer une référence commune à tous les membres de l'équipe projet. Il permettra d'assurer une bonne cohérence et une homogénéité dans les méthodes de travail.
- Donner au projet l'assurance de la sécurité des prestations réalisées tout au long du contrat.
- Identifier tous les acteurs réels du projet.
- Fixer les droits, devoirs et responsabilités du projet, de ses membres, et des éventuels prestataires.
- Indiquer tous les moyens possibles pour répondre aux exigences techniques et sécurités.
- Assurer la cohérence des travaux menés dans le cadre de ce projet.
- Définir les procédures à suivre, les outils à utiliser, les normes à respecter, la méthodologie de développement du produit et les contrôles prévus pour chaque activité.

Il constitue :

- Un outil de travail et un référentiel commun à tous les acteurs pour leur donner une vision similaire du projet.
- Le cahier des charges de la sécurité du projet, réalisé en collaboration avec le client et approuvé par lui.

Chaque partie se doit donc de le respecter.

SECTION 2 - DOCUMENTS DE RÉFÉRENCE

Le référentiel documentaire est constitué notamment par :

- Le Contrat
- Les devis et/ou la proposition commerciale
- L'accord de niveau de service (SLA)
- Conditions Générales de Vente (CGV)
- Ouverture de Compte Client (OCC)
- PSSI IS HDS
- PGSI Groupe OT
- DDA IS HDS / DDAS IS HDS
- Le Plan d'Assurance Sécurité (PAS)
- Les Procès-Verbaux de Recette
- Le Cahier d'Exploitation : remplacé par le dossier d'architecture
- La Matrice de Flux : En cours de rédaction

La liste des documents applicables et de référence n'est pas exhaustive et peut évoluer selon les contextes client.

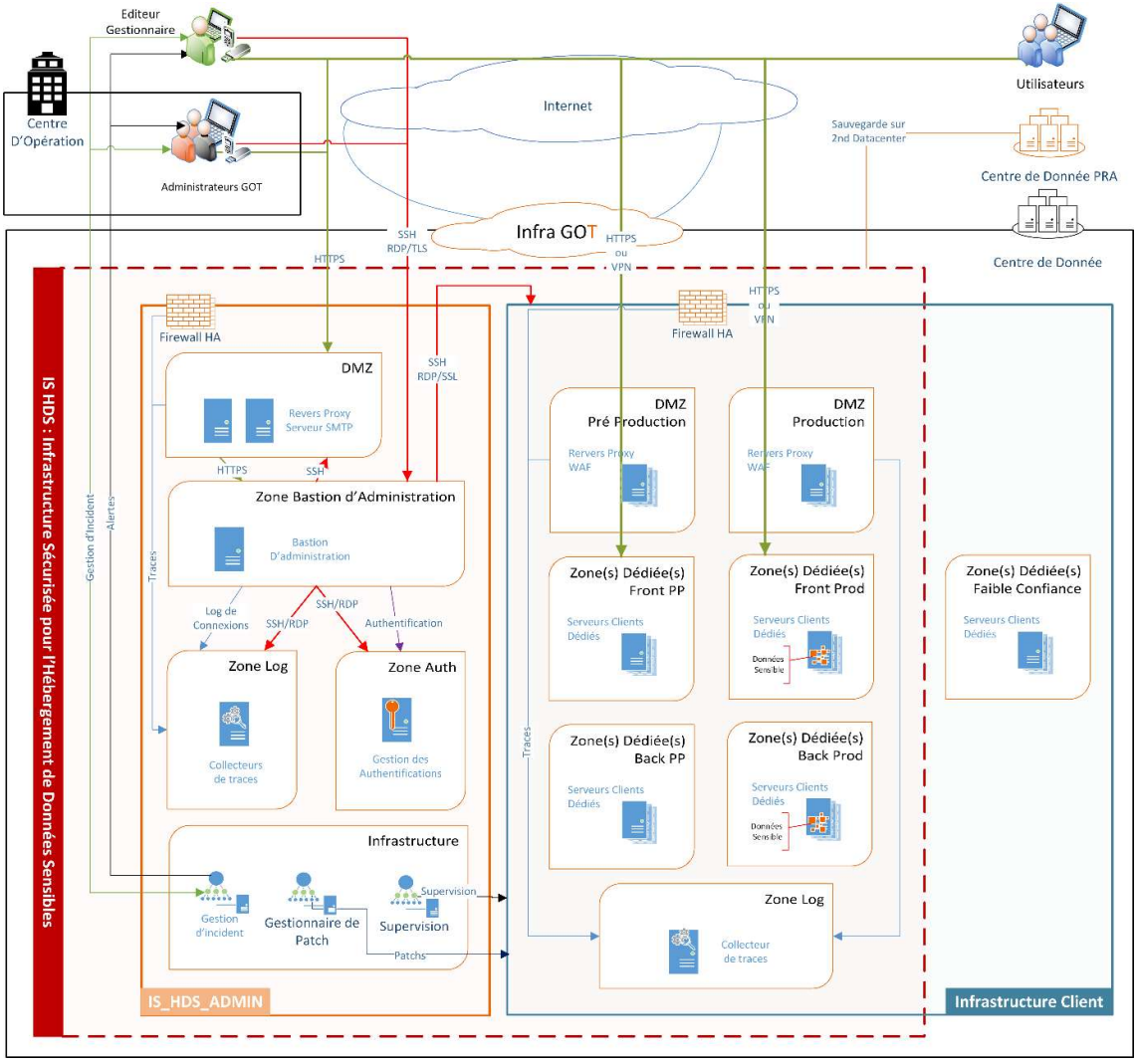
SECTION 3 - DESCRIPTION DU SYSTÈME EXTERNALITÉ

1 - Principe de l'Infrastructure IS-HDS

L'infrastructure sécurisée pour l'hébergement de données sensibles propose la mise en œuvre de mesures de sécurité nominales et de bonnes pratiques issues de l'ISO 27001 et permet de traiter les risques sur les traitements et les données sensibles hébergés.

Le synoptique ci-dessous représente l'infrastructure IS HDS avec les différentes mesures de sécurité encadrant l'organisation des environnements applicatifs, les principaux composants de sécurité, les flux entre les différentes zones.

L'ensemble des clients hébergés sur le périmètre IS HDS doit respecter à minima les mesures de sécurité détaillées par la suite et illustrées sur ce schéma.



2 - Description du système hébergé

2.1 - Introduction

Le client est une Startup qui appartient au Groupe INVERTURE.

Editeur logiciel dont le métier est les essais cliniques. Saisie des entrevus médecins et patients, médicaments, collecte d'infos auprès des patients. Besoin d'être hébergé HDS.

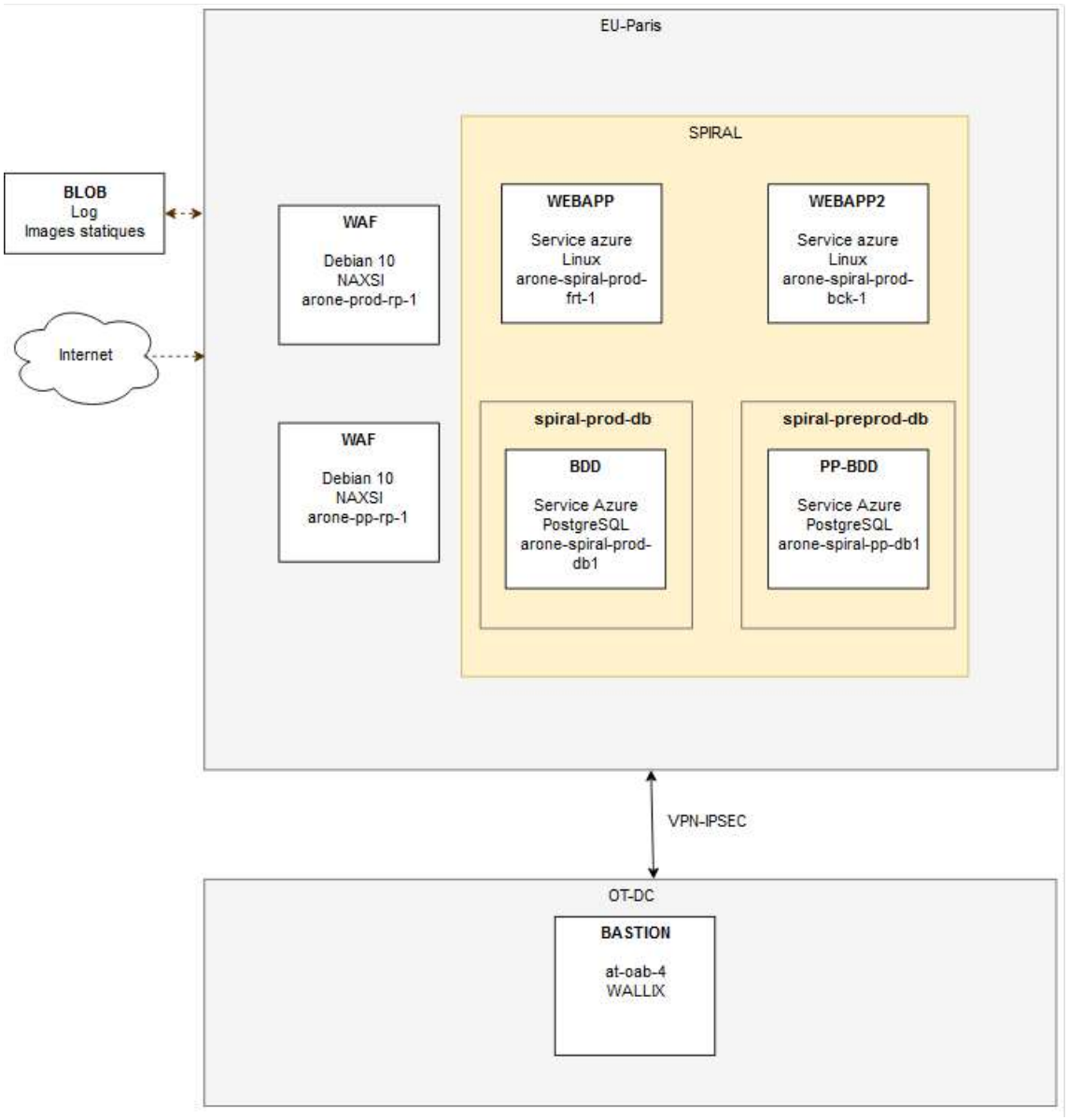
En cible l'infrastructure sera décomposée en 4 plates-formes :

- Socle HDS (déployée)
- Projet SPIRAL (déployée)
- Projet OPAL (à planifier)
- Projet MIGRATION (à planifier)

2.2 - Contexte technique

Cloud	AZURE
Région	France central
ISO 27001	oui - HDS
Haute-disponibilité	non
Autoscaling	non
Firewall applicatif	NAXSI
Bastion de sécurité	Wallix
Tracabilité activité tenant	Azure Monitor
Collecteur de logs	Blob Storage
Environnements	(1) production (1) preproduction
Astreinte 24/7	Non Souscrit
Livraison applicative	Via github sur la préproduction. Processus à déterminer en production.
CI/CD	Oui en préproduction
Fourniture certificat SSL	Certificat SSL Thawte Wildcard
Backup retention	30 jours

2.3 - Schéma


EU-Paris
SPIRAL
BLOB
Log
Images statiques
Internet
WAF
Debian 10
NAXSI
arone-prod-rp-1
WAF
Debian 10
NAXSI
arone-pp-rp-1
WEBAPP
Service azure
Linux
arone-spiral-prod-frt-1
WEBAPP2
Service azure
Linux
arone-spiral-prod-bck-1
spiral-prod-db
BDD
Service Azure
PostgreSQL
arone-spiral-prod-db1
spiral-preprod-db
PP-BDD
Service Azure
PostgreSQL
arone-spiral-pp-db1
VPN-IPSEC
OT-DC
BASTION
at-oab-4
WALLIX

SECTION 4 - RAPPEL DES EXIGENCES DE SÉCURITÉ

2.4 - Exigences de sécurité nominales et Référentiel de sécurité du Groupe OT

Le référentiel de sécurité du Groupe OT décrit le fonctionnement du SMSI (Système de Management de la Sécurité de l'Information) ainsi que les exigences de sécurité nominales appliquées à l'infrastructure de sécurité pour l'hébergement de donnée sensible (IS HDS).

La [PGSI_GROUPEOT] constitue la politique de gouvernance de la sécurité de l'information déployée par le Groupe OT pour sécuriser les données de production confiées par ses clients, ou qui sont traitées par eux au travers des logiciels que le GROUPE OT héberge. Il adresse en particulier les processus d'hébergement, mais également l'ensemble des activités en soutien concernées.

La déclaration d'applicabilité [DDA_ISHDS] décrit les objectifs de sécurité, ainsi que les mesures appropriées et applicables au SMSI du Groupe OT ainsi qu'à la plateforme IS HDS sur laquelle reposent les hébergements sécurisés.

La politique de sécurité des systèmes d'information [PSSI_ISHDS] exprime les règles de sécurité mise en œuvre sur le périmètre.

Notre infrastructure sécurisée est en amélioration continue et fait l'objet d'une analyse de risque mis à jour annuellement.

2.5 - Exigences de sécurité lie à la protection des données personnelles (RGPD)

Le règlement général européen sur la protection des données **(UE) 2016/679** du 24 mai 2016 est applicable au 25 mai 2018. Il consacre une logique de responsabilisation de tous les acteurs impliqués dans le traitement des données personnelles, dès lors qu'elles concernent des résidents européens, que ces acteurs soient ou non établis au sein de l'UE. Il impose des obligations spécifiques aux sous-traitants qui doivent notamment aider les responsables de traitement dans leur démarche permanente de mise en conformité de leurs traitements.

Les exigences de sécurité nominale ainsi que les conditions générales de ventes (CGV) tiennent compte des législations en vigueur et notamment du RGPD **(UE) 2016/679**.

La CNIL édite un « Guide du sous-traitant » qui exprime, notamment, les exigences spécifiques liées aux traitements des données personnelles.

« L'Article 28 - sous-traitant » du règlement spécifie les obligations de chaque partie. Il est rappelé que le client doit documenter les instructions de traitement qu'il confit au prestataire. Notamment il devra lister les traitements qu'il sous-traite au prestataire ainsi que les données personnelles concernées afin que le prestataire puisse maintenir son registre de traitement de sous-traitance.

Selon la nature des données personnelles et des traitements réalisés, une étude d'impact ou analyse de risque doit être menée par le responsable de traitement. Les exigences de sécurité spécifiques qui en résulteraient doivent être communiquées au prestataire pour que ce dernier soit fort de conseil et adapte sa réponse.

Le cahier des charges constitue le point de départ d'une réponse adaptée et circonstanciée et permet au prestataire de remplir son obligation de conseil vis-à-vis du client.

2.6 - Qualifications « sécurité » du Groupe OT

2.6.1 - ISO 27001:2017

Le Groupe OT est certifié ISO 27001:2017.

Le système de management de la sécurité de l'information (SMSI) porte sur la mise à disposition d'une infrastructure sécurisée pour l'hébergement de données sensibles (IS HDS). Ceci en conformité avec la Déclaration d'Applicabilité.

La solution d'hébergement proposée est incluse dans le périmètre de certification.

3 - Exigences de sécurité spécifiques

☒Le client **n'a pas** exprimé d'exigence particulière.

- Seul les exigences de sécurité nominale sont appliquées.
- Les mesures nominales sont précisées dans la section ci-après « Mesures de sécurité nominales ».
- La matrice de couverture est exprimée dans la déclaration d'applicabilité DDA ISHDS.

Ou

☐Le client a exprimé des exigences de sécurité particulières.

- Celles-ci sont décrites dans le document : _____
- Les modalités de mise en œuvre pouvant conduire à un plan d'action spécifique et une facturation particulière. Une étude spécifique a été menée en **avant-projet** avec un chef de projet sécurité du prestataire.
- Les mesures spécifiques en réponse aux exigences exprimées sont détaillées à la section ci-après « Mesures de sécurité spécifiques » et viennent compléter les mesures nominales mises en œuvre sur la plateforme IS HDS.
- La matrice de couverture spécifique est exprimée à la section « Matrice de couverture des exigences de sécurité spécifiques ».

SECTION 5 - ORGANISATION

Chacune des Parties nomme au sein de son organisation des interlocuteurs en charge du projet, le maintien à jour de cette liste est de la responsabilité des Parties, le changement d'interlocuteur ou le départ d'un interlocuteur doit être communiqué dans les meilleurs délais à l'autre Partie.

1 - Organisation de la maîtrise d'œuvre

La Politique de Gouvernance de la Sécurité de l'Information du Groupe OT [PGSI_GroupeOT] est liée au présent PAS. Elle décrit en autre l'organisation mise en œuvre par le Groupe OT pour adresser la sécurité des systèmes d'informations dans le cadre de sa certification ISO 27001.

1.1 - Interlocuteur spécifique au projet

Fonction	Description de la fonction
Chef de Projet	Interlocuteur opérationnel privilégié en charge du projet et responsable : • du pilotage opérationnel du projet ; • de l'organisation des réunions du comité technique et du comité de projet, de la sollicitation du comité de pilotage ou de toute autre réunion nécessaire au bon avancement du projet, notamment réunions de présentation et de validation ; • de l'information des participants de l'entreprise au projet pour ce qui concerne le contexte, les objectifs et l'avancement du projet ; • de la communication aux équipes du Client des documentations de la prestation de service du Groupe OT ; • de la rédaction de tous documents (spécifications, comptes rendus…) ; • de la rédaction des documents de recette. Il est de sa responsabilité d'être attentif au bon déroulement de la prestation de service.
Chef de projet Sécurité	Interlocuteur privilégié pour tous les aspects concernant la mise en œuvre de la sécurité sur le projet, ceci concerne notamment : • la rédaction et le maintien du Plan d'Assurance Sécurité ; • le support à tous les processus du projet ; • le contrôle de la bonne application du PAS sur le projet par l'intermédiaire de revues régulières ; • un support au suivi des risques du projet. Le chef de projet sécurité fait partie de l'équipe projet, le chef de projet coordonne le travail de cet expert avec les autres experts techniques du groupe. Il est en liaison directe avec le RSSI du Groupe OT. Les responsables en charge de la mise en œuvre des différentes règles de sécurité l'assistent autant que de besoin.

1.2 - Autres interlocuteurs liés à la sécurité

Fonction	Description de la fonction
RSSI	Responsable sécurité des systèmes d'information. Il est en charge du maintien et de l'animation du SMSI (Système de management de la sécurité de l'information).
DPD / DPO	Délégué à la protection des données. Il est en charge de mettre en œuvre la conformité au règlement européen sur la protection des données.
Service Delivery Manager	Interlocuteur privilégié en charge de la gestion du contrat de service et responsable : • du respect des engagements de niveaux de services • de l'élaboration d'indicateurs de suivi du projet • des évolutions des documents contractuels • de l'animation des Comités de Pilotage • de l'accompagnement du Client dans la gouvernance du projet Il est de sa responsabilité de suivre les engagements de niveaux de services.

2 - Organisation de la maîtrise d'ouvrage

2.1 - Interlocuteur spécifique au projet

Fonction	Description de la fonction
Représentant de la Direction Générale	Responsable de la maîtrise d'ouvrage globale du projet Rôle d'arbitre et de décisionnaire de la Maîtrise d'Ouvrage
Représentant de la Direction des Systèmes d'Information	Responsable de la Maîtrise d'œuvre Signataire des procès-verbaux de recette
Chef de Projet	Interlocuteur privilégié des intervenants du prestataire en charge du projet Responsable : • du pilotage du projet ; • de l'établissement des ordres de service ; • de la communication à la maitrise d'œuvre des documentations, dossiers utiles à la prestation de service de la maitrise d'œuvre et dans les délais convenant à cette prestation de service ; • de la validation de tous documents (spécifications, comptes rendus…) • de la recette. Il doit informer conformément à l'engagement contractuel le chef de projet de la maitrise d'œuvre, en cas de problèmes concernant le contenu technique de la prestation de service avec communication aux responsables sécurité respectifs, en cas de problèmes relevant de la maîtrise de la sécurité.

2.2 - Autres interlocuteurs liés à la sécurité

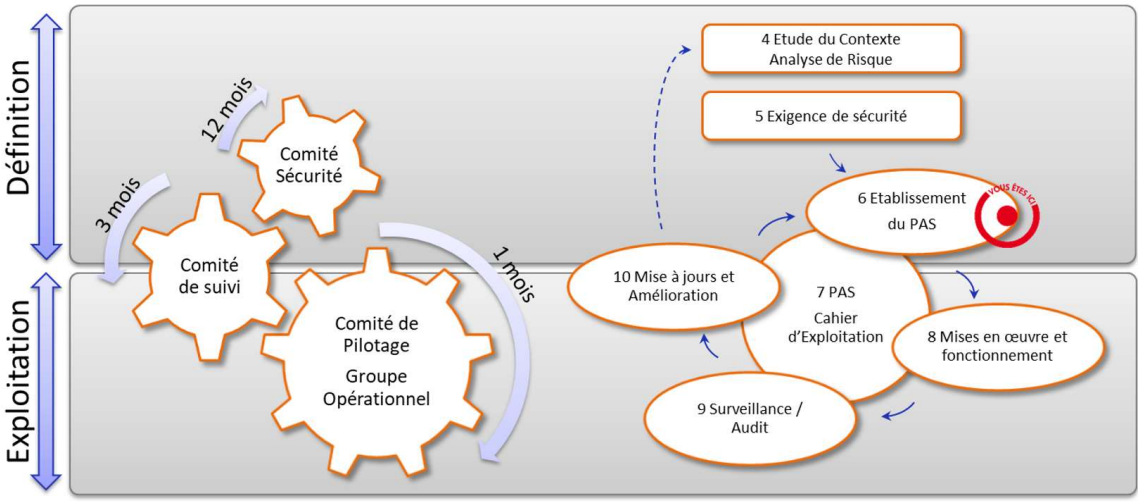
Fonction	Description de la fonction
RSSI	Responsable sécurité des systèmes d'information du client. Il est en charge du maintien et de l'animation de la sécurité chez le client.
DPD / DPO	Délégué à la protection des données du client. Il est en charge de mettre en œuvre la conformité au règlement européen sur la protection des données au sein de l'organisme s'agissant de l'ensemble des traitements mis en œuvre par le client.

3 - Équipe sécurité du projet

L'équipe sécurité du projet est constituée des personnes suivantes :

- Chef de projet Sécurité du Client
- Chef de projet Sécurité du prestataire
- Chef de projet Client
- Chef de projet du prestataire

4 - Instances de suivi de la sécurité du projet



- Au quotidien, le suivi de la sécurité du projet est assuré par le chef de projet du prestataire qui intègre des points sécurités lors des comités de pilotage/groupe opérationnel et comité de suivi.
- Un comité de sécurité est organisé au moins annuellement pour revoir le PAS et l'amender.

Comité de sécurité	
Objet :	C'est l'instance sécuritaire du projet. Il assure la maîtrise sécuritaire du projet et réalise une projection stratégique en tenant compte des risques, des évolutions législatives et évolutions des bonnes pratiques.
Périodicité :	Annuelle
Ordre du jour :	• Stratégie Sécurité des deux parties • Revue du PAS • Revue des évolutions normatives et législatives • Relevé des décisions et actions à engager
Durée	Selon actualité
Participants à minima :	Équipe sécurité : • Chef de projet Sécurité du Client • Chef de projet Sécurité du prestataire • Le chef de projet Client • Le chef de projet du prestataire
ANIMATION / Rédaction du CR :	Animation : Chef de projet du prestataire - Rédaction : Chef de projet du prestataire
Diffusion du CR :	Il est diffusé aux participants ainsi qu'au comité de suivi pour prise en compte des actions sécurité à mener.
Validation du CR :	Ce compte-rendu doit faire l'objet de remarques écrites ou être approuvé par les membres du comité de sécurité sous 10 jours ouvrés après remise. Sans remarques sous 10 jours ouvrés, le compte-rendu est considéré comme validé.

SECTION 6 - ÉLABORATION, ÉVOLUTIONS ET DÉROGATIONS AU PLAN D'ASSURANCE SÉCURITÉ

1 - Élaboration, validation et approbation du PAS

L'établissement et les mises à jour du plan ainsi que le suivi de son application sont de la responsabilité du chef de projet sécurité avec la validation d'un Responsable de la Sécurité du Système d'Information du prestataire (RSSI).

L'approbation formelle du PAS par le client est requise.

2 - Procédure d'évolution du PAS

Les mises à jour du plan doivent être justifiées par une amélioration des conditions de déroulement du projet ou de la sécurité des fournitures. Toute évolution doit être référencée dans le suivi des versions et dans l'état des mises à jour.

Voici une liste non exhaustive des situations susceptibles d'entraîner une modification du PAS :

- Évolution du système d'information (configuration logicielle ou matérielle) ;
- Évolution de l'environnement du système d'information (locaux, personnels, procédures, etc.) ;
- Évolution du périmètre de l'opération.
- Évolution des obligations légales.
- Évolution normative.

3 - Diffusion du PAS

Une fois approuvé, le PAS est applicable et diffusé à tous les acteurs du projet.

Le chef de projet sécurité du prestataire est responsable de la diffusion du PAS au sein de son organisation et auprès de ses sous-traitants éventuels.

Le chef de projet sécurité du client est responsable de la diffusion du PAS auprès de ces propres équipes et des autres parties prenantes le cas échéant (éditeur, intégrateur, auditeur, client final).

4 - Applicabilité du PAS

Chaque membre participant à la mise en œuvre de ce projet (client, hébergeur, éditeur, intégrateur, auditeur) doit se conformer au PAS.

5 - Non-application du PAS

La non-application de dispositions du PAS est justifiée par une dérogation.

La non-application de dispositions du PAS non justifiée par une dérogation constitue un écart.

Un acteur du projet identifiant un écart doit en référer immédiatement auprès chef de projet référent qui le remontra au chef de projet sécurité du prestataire.

Selon la gravité de l'écart, la procédure de gestion d'incident de sécurité du prestataire est déclenchée.

Le client et les responsables concernés sont notifiés, l'écart fera l'objet d'un point particulier lors du comité de pilotage suivant.

Les dispositions sont alors prises par l'équipe sécurité avec l'appui éventuel des RSSI et DPD pour :

- Faire respecter les procédures,
- Mener les actions correctives nécessaires pour lever l'écart,
- Faire évoluer le PAS,
- Établir ou faire établir une demande de dérogation.

6 - Demande de dérogation

Un acteur du projet n'étant pas à même de remplir l'ensemble des clauses du PAS devra effectuer une demande de dérogation auprès du chef de son chef projet sécurité référent.

La demande de dérogation de Sécurité SI a un caractère exceptionnel et ponctuel ; elle est revue à la date de fin de dérogation et au minimum tous les ans.

La dérogation SSI peut concerner :

- Le non-respect d'une ou plusieurs dispositions définies et validées dans le PAS,
- Une demande de livraison d'un produit non conforme (exemple : livraison d'un lot de logiciels contenant des anomalies identifiées, mais non clôturées).

La demande est étudiée par les chefs de projet sécurité et validée par les RSSI du prestataire et du client.

Si la demande de dérogation impacte la sécurité d'un traitement de données personnelles, les DPD (Délégué à la Protection des Données), ou à défaut les directions, de tous les parties devront approuver la dérogation.

Dans tous les cas, la demande et la décision sont notifiées au demandeur après enregistrement de la décision.

Les dérogations sont enregistrées en annexe du présent PAS.

La durée de la dérogation autorisée sera précisée systématiquement. Une dérogation n'est jamais permanente et sera revue au moins annuellement.

SECTION 7 - MESURES DE SÉCURITÉ

Les mesures spécifiques viennent en réponse aux exigences de sécurité exprimée par le client.

1 - Mesures de sécurité nominales

1.1 - Politique de sécurité

REG_PAS_1 : L'organisation de la sécurité chez le prestataire est décrite dans le document chapeau Politique de Gouvernance de la Sécurité de l'information du Groupe OT [PGSI_GROUPEOT].

REG_PAS_2 : Les mesures nominales de sécurité sont dictées par la Politique de Sécurité du Système d'Information IS HDS [PSSI_IS_HDS] rédigée et mise à jour par le prestataire.

REG_PAS_3 : La [PSSI_IS_HDS] est mise à jour annuellement (elle est consultable sur le site OT dans le cadre d'un audit).

Les mesures suivantes concernent directement les infrastructures IS HDS.

1.2 - Interlocuteurs spécifiques au projet

REG_PAS_4 : Le projet est piloté par un chef de projet, ces fonctions sont décrites dans le présent PAS.

REG_PAS_5 : Un chef de projet sécurité est rattaché au projet, ces fonctions sont décrites dans le présent PAS.

1.3 - Plan d'Assurance Sécurité

REG_PAS_6 : Un plan d'assurance sécurité est mis en œuvre, il décrit les dispositions de sécurité particulières du projet, réputées satisfaire les exigences des partenaires du projet en matière de sécurité, définie en accord avec le client.

Le PAS est maintenu par le chef de projet sécurité du prestataire.

1.4 - Documentations

REG_PAS_8 : Le projet doit documenter à minima un cahier d'exploitation et une matrice de flux. En cours

Le maintien de cette documentation est réalisé par le chef de projet du prestataire.

1.5 - Pilotage

REG_PAS_9 : Différentes instances de suivi sont mises en place et organisées par le chef de projet du prestataire tel que défini dans le présent PAS.

1.6 - Infogérance

REG_PAS_10 : La plateforme est info gérée par le prestataire.

REG_PAS_11 : Tout le personnel du prestataire est géré par des processus d'enrôlement, de désenrôlement et de mutation. Les références et le casier judiciaire sont vérifiés dans le processus.

1.7 - Astreinte

REG_PAS_12 : L'infrastructure doit être sous astreinte.

REG_PAS_13 : Le client doit être joignable en dehors des heures ouvrées. Une procédure pour joindre le contact responsable chez le client doit être fournie et validée.

1.8 - Gestion des accès

REG_PAS_14 : Les accès sont nominatifs.

REG_PAS_15 : Les actions à privilèges élevés sont journalisées.

REG_PAS_16 : Les accès logiques et les politiques de mots de passe des utilisateurs des applications hébergées sont de la responsabilité du client.

1.9 - Bastion d'administration

REG_PAS_17 : Les accès administrateur du prestataire, du client et de leurs sous-traitants doivent être réalisés au travers d'un bastion d'administration.

Note : pas d'accès admin côté client

REG_PAS_18 : Les identifiants génériques ne sont pas autorisés sur le bastion d'administration. Ils sont à proscrire sur l'ensemble de la plateforme.

1.10 - Sécurité des flux

1.10.1 - Firewall

REG_PAS_19 : L'infrastructure doit disposer de firewalls redondés.

REG_PAS_20 : Les firewalls doivent pouvoir exporter leurs logs vers le serveur syslog dédié de l'infrastructure client.

1.10.2 - DMZ

REG_PAS_21 : L'infrastructure doit disposer de reverse proxy en DMZ pour filtrer les flux en provenance d'internet et à destination du système d'information hébergé.

REG_PAS_22 : Les flux web doivent transiter par un firewall web applicatif (WAF).

1.10.3 - Cloisonnement

REG_PAS_23 : Il ne doit y avoir qu'un seul type de service par serveur.

REG_PAS_24 : L'application, la base de données et le centralisateur de log doivent être sur des serveurs différents dans des vlan différents. ok blob

REG_PAS_25 : Les outils d'administration de l'application (back-office) ne doivent pas être accessibles par les mêmes URL que l'application utilisateur.

1.10.4 - Chiffrement des flux

REG_PAS_26 : Tous les flux échangés au travers d'Internet doivent être chiffrés (SSL, TLS, SSH, VPN).

REG_PAS_27 : Les flux d'administration sont systématiquement chiffrés.

1.10.5 - Système de prévention d'intrusion

REG_PAS_28 : L'IPS doit être activé sur les firewalls.

1.11 - Séparation des environnements

1.11.1 - Zone de faible confiance

REG_PAS_29 : L'évolution de l'infrastructure client historique vers une infrastructure sécurisée implique de conserver dans une zone (vlans) séparé dites de faible confiance :

- Des systèmes en attente de migration vers l'infrastructure sécurisée.
- Des systèmes obsolètes ne disposant plus de licence, contrat de maintenance ou de mise à jour de sécurités.
- Des systèmes dont les services ne peuvent pas être cloisonnés.
- Des systèmes que le client ne souhaite pas intégrer à l'infrastructure sécurisée.

- Pas encore migré

1.11.2 - Pré-production

REG_PAS_30 : Avant la mise en production, tout déploiement est contrôlé et validé sur l'environnement de pré production client qui est *iso* fonctionnel de l'environnement de production client.

1.12 - Antivirus

REG_PAS_31 : Une solution antivirus/antimalware doit être mise en œuvre pour vérifier les fichiers en provenance d'internet à minima. N/A car aucune PJ uploadée

L'antivirus peut être positionné sur le firewall ou les reverse proxy dès lors qu'il a accès aux pièces jointes.

1.13 - Centralisation des logs

REG_PAS_32 : Les logs sont centralisés sur un serveur dédié à la plateforme. BLOB Azure sf FW

Ces derniers pourront alimenter l'outil de sécurité ban-manager du prestataire.

1.14 - Mise à jour

REG_PAS_33 : La mise à jour des systèmes et de ses composants est automatique.

Si le client souhaite une mise à jour manuelle, un protocole de gestion des patchs doit être étudié, documenté et validé par les RSSI du prestataire et du client.

REG_PAS_34 : Les mises à jour des composants applicatifs fournis par le client ou l'un de ses sous-traitants sont de la responsabilité du client. réalisation de la maj par OT

1.15 - Continuité d'activité

REG_PAS_35 : L'infrastructure dispose à minima d'un plan de sauvegarde sur un second site géographique.

1.16 - Test de vulnérabilité

REG_PAS_36 : Le prestataire conduit des tests de vulnérabilités périodiques pour vérifier l'exposition de la plateforme sur Internet.

1.17 - Test de sécurité

REG_PAS_37 : Le client à la charge de réaliser un test de sécurité avant la mise en production initiale puis annuellement ou après chaque évolution majeure. Un protocole de test de sécurité impliquant toutes les parties prenantes (client, auditeur, éditeur, hébergeur) doit être signé à ces occasions.

L'équipe sécurité du projet aura pour mission de planifier la correction des écarts identifiés.

2 - Mesures de sécurité spécifiques

Les mesures de sécurité spécifiques ci-dessous répondent aux exigences de sécurités spécifiques du projet exprimer par le client.

Le client n'a pas exprimé d'exigence de sécurité spécifique.

REG_PAS_xx : Sauvegardes ??

SECTION 8 - COUVERTURE DES EXIGENCES DE SÉCURITÉ

1 - Couverture des exigences de sécurité nominales

La matrice de couverture des exigences de sécurité nominales est la déclaration d'applicabilité [DDA_ISHDS] sur laquelle repose la certification ISO 27001 du Groupe OT. Cette dernière fait l'objet d'un audit de maintien de certification annuel.

Une version simplifiée est mise à disposition sur demande [DDAS_ISHDS]. La version complète peut être auditée sur site.

2 - Couverture des mesures pour traiter les risques sur les libertés et la vie privée (RGPD)

Dans le cadre du RGPD, la CNIL propose un catalogue de bonnes pratiques « Mesures pour traiter les risques sur les libertés et la vie privée ». La matrice de correspondance avec l'annexe A et l'ISO 27001 et donc avec la [DDA_ISHDS] précitée est proposée en annexe du présent document.

3 - Couverture des exigences de sécurité spécifiques

Le tableau suivant détaille le niveau de couverture des mesures mises en œuvre pour répondre aux exigences spécifiques émise par le donneur d'ordre le cas échéant.

Exigence spécifique	Ref mesures misent en œuvre	Couverture

SECTION 9 - ANNEXES

1 - Dérogations actives

1.1 - L'infrastructure n'est pas sous astreinte

Intitulé	L'infrastructure n'est pas sous astreinte
Règle(s) dérogé(s)	REG_PAS_12
Système(s) cible(s)	Environnement de production
Concerne un traitement de données personnel	Non
Origine de la demande	Client
Date de 1er dérogation	11/2021
Dernière date de renouvellement	
Date butoir (Max renouvellement + 1 an)	11/2022
Risques encourus	Délai d'intervention en cas d'incident sur la plateforme
Justification	Demande du client
Condition de mise en oeuvre	
Contournement	N/A
Validateurs, entités et fonctions	RSSI OT, RSSI client

1.2 - Client non joignable en dehors des heures ouvrables

Intitulé	Le client n'est pas joignable en dehors des heures ouvrables
Règle(s) dérogé(s)	REG_PAS_13
Système(s) cible(s)	Environnement de production
Concerne un traitement de données personnel	Non
Origine de la demande	Client
Date de 1er dérogation	11/2021
Dernière date de renouvellement	
Date butoir (Max renouvellement + 1 an)	11/2022
Risques encourus	Impossibilité de contacter le client en HNO en cas d'incident
Justification	Demande du client
Condition de mise en oeuvre	
Contournement	N/A
Validateurs, entités et fonctions	RSSI OT, RSSI client

1.3 - Pas d'export des logs FW sur un Syslog centralisé

Intitulé	Les FW doivent exporter leurs logs vers un Syslog dédié de la plateforme
Règle(s) dérogé(s)	Reg_PAS_20
Système(s) cible(s)	Environnement de production
Concerne un traitement de données personnel	Non
Origine de la demande	
Date de 1er dérogation	11/2021
Dernière date de renouvellement	
Date butoir (Max renouvellement + 1 an)	11/2022
Risques encourus	Risque de perte des logs en cas de crash du serveur
Justification	
Condition de mise en oeuvre	Les logs sont conservés localement sur le serveur pendant 366 jours
Contournement	Les logs sont cependant sauvegardés avec les backups du serveur (30 jours)
Validateurs, entités et fonctions	RSSI OT, RSSI client

1.4 - l'IPS n'est pas activé

Intitulé	L'IPS doit être activé sur les FW
Règle(s) dérogé(s)	Reg_PAS_28
Système(s) cible(s)	Environnement de production
Concerne un traitement de données personnel	Non
Origine de la demande	
Date de 1er dérogation	11/2021
Dernière date de renouvellement	
Date butoir (Max renouvellement + 1 an)	11/2022
Risques encourus	Risque d'intrusion sur la plateforme
Justification	
Condition de mise en oeuvre	Il n'y a pas d'IPS devant la plateforme
Contournement	La plateforme se trouve derrière naxsi ce qui la protège en partir (au niveau applicatif)
Validateurs, entités et fonctions	RSSI OT, RSSI client

1.5 - Sauvegarde sur un second site géographique.

Intitulé	Pas de redondance géographique des sauvegardes
Règle(s) dérogé(s)	REG_PAS_35
Système(s) cible(s)	Environnement de production
Concerne un traitement de données personnel	Non
Origine de la demande	
Date de 1er dérogation	11/2021
Dernière date de renouvellement	
Date butoir (Max renouvellement + 1 an)	11/2022
Risques encourus	Risque de perte des données en cas d'incident majeur sur le site principal
Justification	
Condition de mise en oeuvre	Le stockage est localement redondant (LRS : copie des données 3 fois), mais sur un même emplacement physique
Contournement	
Validateurs, entités et fonctions	RSSI OT, RSSI client

1.6 - Absence de test de sécurité avant la mise en production initiale

Intitulé	Absence de réalisation d'un test de sécurité avant la mise en production initiale
Règle(s) dérogé(s)	REG_PAS_37
Système(s) cible(s)	Environnement de production
Concerne un traitement de données personnel	Non
Origine de la demande	Client
Date de 1er dérogation	11/2021
Dernière date de renouvellement	
Date butoir (Max renouvellement + 1 an)	12/2021
Risques encourus	Risque de présence de failles de sécurité pouvant compromettre la sécurité de la plateforme
Justification	Demande du client
Condition de mise en oeuvre	
Contournement	
Validateurs, entités et fonctions	RSSI OT, RSSI client

2 - Correspondance des mesures pour traiter les risques sur les DCP et l'Annexe A de l'ISO 27001:2017

RGPD : Mesures pour traiter les risques sur les libertés et la vie privée		Principales correspondances Annexe ISO 27001:2017	
1. Agir sur les éléments à protéger			
1.1	1. Minimiser les DCP	A 18.1.4	Conformité / Protection de la vie privée et protection des données à caractère personnel
1.2	2. Gérer les durées de conservation des DCP		
1.3	3. Informer les personnes concernées		
1.4	4. Obtenir le consentement des personnes concernées		
1.5	5. Permettre l'exercice du droit d'opposition		
1.6	6. Permettre l'exercice du droit d'accès direct		
1.7	7. Permettre l'exercice du droit de rectification		
1.8	8. Cloisonner les DCP	A 9.2	Gestion de l'accès utilisateur
		A 9.4	Contrôle de l'accès au système et à l'information
1.9	9. Chiffrer les DCP	A 10.1	Mesures cryptographiques
		A 13.1.2	Sécurité des services de réseau
1.10	10. Anonymiser les DCP	A 18.1.4	Conformité / Protection de la vie privée et protection des données à caractère personnel
2. Agir sur les impacts			
2.1	11. Sauvegarder les DCP	A 12.3.1	Sauvegarde des informations
2.2	12. Protéger les archives de DCP	A 12.3.1	Sauvegarde des informations
2.3	13. Contrôler l'intégrité des DCP	A 10.1	Mesures cryptographiques
2.4	14. Tracer l'activité sur le système informatique	A 12.4	Journalisation et surveillance
2.5	15. Gérer les violations de DCP	A 16.1	Gestion des incidents liés à la sécurité de l'information et améliorations
3. Agir sur les sources de risques			
3.1	16. S'éloigner des sources de risques	A 11.1	Zones sécurisées
3.2	17. Marquer les documents contenant des DCP	A 8.2	Classification de l'information
3.3	18. Gérer les personnes internes qui ont un accès légitime	A 6.1	Organisation interne
		A 7	La sécurité des ressources humaines
3.4	19. Contrôler l'accès logique des personnes	A 9.2	Gestion de l'accès utilisateur

RGPD : Mesures pour traiter les risques sur les libertés et la vie privée		Principales correspondances Annexe ISO 27001:2017	
		A 9.4	Contrôle de l'accès au système et à l'information
		A 10.1	Mesures cryptographiques
3.5	20. Gérer les tiers qui ont un accès légitime aux DCP	A 15.1	Sécurité de l'information dans les relations avec les fournisseurs
3.6	21. Lutter contre les codes malveillants	A 12.2	Protection contre les logiciels malveillants
3.7	22. Contrôler l'accès physique des personnes	A 11.1	Zones sécurisées
3.8	23. Se protéger contre les sources de risques non humaines	A 11.1	Zones sécurisées
		A 13.1	Management de la sécurité des réseaux
4. Agir sur les supports			
4.1	24. Réduire les vulnérabilités des logiciels	A 12.2	Protection contre les logiciels malveillants
		A 12.5	Maîtrise des logiciels en exploitation
		A 12.6	Gestion des vulnérabilités techniques
		A 14.2	Sécurité des processus de développement et d'assistance technique
4.2	25. Réduire les vulnérabilités des matériels	A 8.1	Responsabilités relatives aux actifs
		A 8.3	Manipulation des supports
		A 11.1	Zones sécurisées
		A 11.2	Matériels
		A 12.1.3	Dimensionnement
4.3	26. Réduire les vulnérabilités des canaux informatiques	A 11.1	Zones sécurisées
		A 13.1	Management de la sécurité des réseaux
		A 13.2	Transfert de l'information
4.4	27. Réduire les vulnérabilités des personnes	A 7	La sécurité des ressources humaines
4.5	28. Réduire les vulnérabilités des documents papier	A 8	Gestion des actifs
		A 8.3.2	Mise au rebut des supports
4.6	29. Réduire les vulnérabilités des canaux papier	A 8	Gestion des actifs
5. Actions transverses (au niveau de l'organisme)			

RGPD : Mesures pour traiter les risques sur les libertés et la vie privée		Principales correspondances Annexe ISO 27001:2017	
5.1	30. Gérer l'organisation de protection de la vie privée	A 6	Organisation de la sécurité de l'information
5.2	31. Gérer les risques sur la vie privée	A 6	Organisation de la sécurité de l'information
5.3	32. Gérer la politique de protection de la vie privée	A 5.1.1	Politiques de sécurité de l'information
5.4	33. Intégrer la protection de la vie privée dans les projets	A 6.1.5	La sécurité de l'information dans la gestion de projet
		A 12.1.2	Gestion des changements
		A 14	Acquisition, développement et maintenance des systèmes d'information
5.5	34. Superviser la protection de la vie privée	A 18.1.4	Conformité / Protection de la vie privée et protection des données à caractère personnel
		A 18.2	Revue de la sécurité de l'information