

Sécurité dans la relation avec les Fournisseurs

DSN/SSI

1.3

C1 – Interne

En cours

Table des matières

1	FICHE DE SUIVI	3
1.1	HISTORIQUE DES MODIFICATIONS	3
2	OBJECTIFS.....	4
3	PERIMETRE D'APPLICATION.....	4
4	DESCRIPTION	5
4.1	SECURITE DE L'INFORMATION DANS LES RELATIONS AVEC LES FOURNISSEURS	5
4.2	SURVEILLANCE, AUDIT ET REVUE DES FOURNISSEURS	6
5	EXIGENCES DE SECURITE	8
5.1	PROTECTION DES DONNEES PERSONNELLES.....	8
5.2	CONFIDENTIALITE	8
5.3	SECURITE.....	9
5.4	LES EXIGENCES FONCTIONNELLES DE SECURITE.....	15
5.5	METHODOLOGIE SECURISEE D'INGENIERIE ET DE DEVELOPPEMENT	17
5.6	GESTION DES EVOLUTIONS	18
5.7	AUDITS.....	18
6	ANNEXES	20
	DEFINITIONS	20
	CHECKLIST	21
	COORDONNEES.....	22
	MATRICE IMPACT-GRAVITE	23
	MODELE DE PLAN D'ASSURANCE SECURITE (PAS).....	24
	MODELE DE QUESTIONNAIRE DE SURVEILLANCE, REVISION ET GESTION DES CHANGEMENTS DES SERVICES FOURNISSEURS – VERSION 3.0	25
	DOCUMENTS DE REFERENCE	27

1 FICHE DE SUIVI

1.1 Historique des modifications

Nom du document	PROC_FournisseurSécurité_V1.2
Prochaine mise à jour	2025
Durée d'utilité administrative	3 ans
Responsable	PERRET Didier
Approbateur	RAMAYE Hubert., GABOREL Sandrine

Suivi des versions			
Version	Date	Auteur	Objet
0.1	03/06/2022	PERRET D.	Création du document
0.2	07/06/2022	PERRET D.	Reprise des documents produits antérieurement.
0.3	08/06/2022	PERRET D.	Traitement des NC 2020-MIN18, 2021-MIN11. Traitement de la NC 2205-MAJ04
0.4	08/06/2022	PERRET D.	Observations émises lors de la réunion du 10/06/2022
0.5	13/06/2022	PERRET D.	Critères d'évaluation de la criticité d'un Fournisseur
0.6	15/06/2022	PERRET D.	Observations émises lors de la réunion du 15/06/2022
0.9	22/06/2022	PERRET D.	Observations émises lors de la réunion du 22/06/2022.
1.0	22/06/2022	BLANC E.	Mise en forme
1.1	02/03/2023	PERRET D.	Revue 2023.
1.11	03/07/2023	PERRET D.	Prise en compte des contrats. Actualisation « 5.3.11 Télémaintenance/Téléassistance »
1.12	02/03/2024	PERRET D.	Revue 2024. Inscription de la revue obligatoire du registre des personnels habilités par le Fournisseur. Indication de l'adresse de messagerie de signalement des failles et incidents de sécurité aphp-signalement-securite@aphp.fr
1.2	22/04/2024	PERRET D.	Traitement des non-conformités mineures CCO-57 et 2402-MIN08. Mise en annexe du Modèle de questionnaire de surveillance, révision et gestion des changements des services fournisseurs - Version 3.0. Intégration du BASTION d'administration WALLIX.
1.3	22/04/2025	PERRET D.	Prise en compte des nouvelles versions des normes ISO 27001, ISO 27002 et du référentiel de certification HDS V2.0 2024

Résumé et mots clefs

Audit, certification, confidentialité, contrat, contrôle, convention, développement, directive, échange, exercice des droits, homologation, imputabilité, journalisation, marché, politique, registre, RGPD, sécurité, secret, sous-traitance, télémaintenance.

2 OBJECTIFS

La présente procédure est prise en application de la DIRECTIVE – Sécurité dans les relations avec les fournisseurs.

Les objectifs de cette procédure sont :

- Garantir la protection des actifs de l'AP-HP accessibles aux Fournisseurs
- Maintenir un niveau convenu de sécurité de l'information et de prestation de services, conformément aux Marchés conclus avec les Fournisseurs ou contrats conclus avec les partenaires.

La procédure décrit le processus de gestion des relations avec les Fournisseurs, les exigences générales minimales de sécurité en réponse à ces objectifs et les modalités de surveillance, d'audit et de revue des Fournisseurs.

3 PÉRIMÈTRE D'APPLICATION

Ce document s'applique à tout le SI de l'APHP.

QUOI			
Système d'Information Essentiel	SI Hébergeur de Données de Santé	SI Biomédicaux et Techniques	Autres SI
✓	✓	✓	✓

QUI				
Patients Usagers	Personnels AP-HP	Professionnels tiers	Étudiants	Fournisseurs
		✓		✓

4 DESCRIPTION

4.1 Sécurité de l'information dans les relations avec les Fournisseurs

L'AP-HP joint aux Marchés et Contrats avec les Fournisseurs les exigences minimales de sécurité de l'information auxquelles les Fournisseurs doivent se conformer pour limiter les risques résultant de l'accès des Fournisseurs aux actifs ou de la fourniture de composants de l'infrastructure informatique de l'AP-HP.

L'[Article 5](#) « Confidentialité - Protection des données personnelles - Mesures de sécurité » du cahier des clauses administratives générales des marchés publics de techniques de l'information et de la communication (CCAG TIC) (NOR : ECOM2106875A) est applicable pour les marchés relevant du CCAG TIC.

L'[Article 5](#) « Confidentialité - Protection des données personnelles - Mesures de sécurité » du cahier des clauses administratives générales des marchés publics de techniques de l'information et de la communication (CCAG FCS) (NOR : ECOM2106868A) est applicable pour les marchés relevant du CCAG FCS.

L'Arrêté du 18 septembre 2018 portant approbation du cahier des clauses simplifiées de cybersécurité (NOR : ECOP1825228A) est applicable.

Le présent document complète et précise les dispositions de l'Article 5 du CCAG TIC et du CCAG FCS ainsi que l'arrêté 18 septembre 2018.

La présente procédure comporte une checklist permettant à l'AP-HP de préciser de manière synthétique le contexte d'intervention du Fournisseur. Cette checklist facilite l'identification par le Fournisseur de ses obligations (Cf. annexe).

Le Fournisseur identifie un point de contact administratif au sein de son organisation qui sera destinataire des notifications de violation de données personnelles pour les personnes concernés qui relèveraient de la responsabilité du Fournisseur ainsi que des questionnaires d'évaluation périodique des prestations de services assurées par les fournisseurs afin de répondre à l'objectif de sécurité « Maintenir le niveau convenu de sécurité de l'information et de service conforme aux accords conclus avec les fournisseurs » de l'annexe A de la norme ISO 27001 : 2017 (ou A. 5.22 de la norme ISO 27001 : 2023).

Le Fournisseur identifie un point de contact technique au sein de son organisation qui sera chargé de gérer les accès aux locaux et aux systèmes d'information de l'AP-HP pour le compte du Fournisseur.

Le processus de gestion des relations avec les Fournisseurs est mis en œuvre par le Pôle d'Intérêt Commun (PIC) AGEPS de l'AP-HP en collaboration avec la Direction des Services Numériques (DSN).

Pour les marchés, le processus achat suit les étapes suivantes :

- Initialisation
- Expression de besoin
- Rédaction du dossier de consultation
- Publication du DCE comportant la documentation spécifique à la sécurité de l'information¹
- Analyse des offres ou négociation selon le type de marché

¹ La documentation spécifique à la sécurité de l'information est constituée de :

- La charte du bon usage du système d'information de l'AP-HP annexe n°16 du règlement intérieur de l'AP-HP
- Politique Générale de Sécurité de l'information (PGSI) de l'AP-HP, les directives de sécurité prises en application de la PGSI de l'AP-HP (Cf. liste en annexe), le cadre de cohérence technique du système d'information de l'AP-HP et la présente procédure.

- Soumission aux instances
- Notification.

Dans le cas des centrales d'achat, le processus achat suit les étapes suivantes :

- Initialisation
- Expression de besoin
- Prospection minutieuse des fournisseurs (SOURCING)
- Négociation
- Soumission aux instances
- Adhésion à l'accord cadre via convention
- Emission d'un courrier à l'attention du Fournisseur comportant la documentation spécifique à la sécurité de l'information de l'AP-HP¹ par le pouvoir d'adjudicateur.

Pour les services, le Fournisseur a l'obligation de diffuser la documentation spécifique à la sécurité de l'information de l'AP-HP jusqu'au dernier maillon de la chaîne d'approvisionnement si le Fournisseur sous-traite des parties des services rendus à l'AP-HP.

Pour les produits informatiques, le Fournisseur a l'obligation de diffuser les pratiques de sécurité appropriées jusqu'au dernier maillon de la chaîne d'approvisionnement si ces produits comportent des composants achetés chez d'autres Fournisseurs.

Les personnels du PIC AGEPS impliqués dans le processus des achats informatiques sont sensibilisés à la sécurité de l'Information.

4.2 Surveillance, Audit et Revue des Fournisseurs

L'AP-HP surveille, revoie et audite à intervalles réguliers les prestations de service assurés par les Fournisseurs afin de s'assurer que les exigences de sécurité de l'information prévues dans les Marchés/Contrats sont bien respectées et que les incidents et les problèmes liés à la sécurité de l'information sont gérés correctement.

Les Fournisseurs ont pour obligation de constituer les preuves de conformité aux exigences de sécurité. L'AP-HP demande la communication de ces preuves dans le cadre de la présente procédure. Le degré de surveillance des Fournisseurs dépend des critères suivants issus de la méthode EBIOS RM.

Exposition			Fiabilité CYBER		
Niveau	Dépendance	Pénétration	Maturité	Confiance	Niveau
1	Relation non nécessaire aux fonctions stratégiques	Pas d'accès ou accès avec privilèges de type utilisateur à des terminaux utilisateurs (poste de travail, téléphone mobile, etc.)	Des règles d'hygiène informatique sont appliquées ponctuellement et non formalisées. La capacité de réaction sur incident est incertaine.	Les intentions de la partie prenante ne peuvent être évaluées	1
2	Relation non utile aux fonctions stratégiques	Accès avec privilèges de type administrateur à des terminaux utilisateurs (parc informatique, flotte de terminaux mobiles, etc.) ou accès physique aux sites de l'organisation	Les règles d'hygiène et la réglementation sont prises en compte sans intégration dans une politique globale. La sécurité numérique est conduite selon un mode réactif.	Les intentions de la partie prenante sont considérées comme neutres	2
3	Relation indispensable mais non exclusive	Accès avec privilèges de type administrateur à des serveurs "métiers" (serveur de fichiers, bases de données, serveur web, serveur d'application, etc.)	Une politique globale est appliquée en matière de sécurité numérique. Celle-ci est assurée selon un mode réactif, avec une recherche de centralisation et d'anticipation sur certains risques.	Les intentions de la partie prenante sont connues et probablement positives	3

Exposition			Fiabilité CYBER		
Niveau	Dépendance	Pénétration	Maturité	Confiance	Niveau
4	Relation indispensable et unique (pas de substitution possible à court terme)	Accès avec privilèges de type administrateur à des équipements d'infrastructures (annuaires, DNS, DHCP, commutateurs, pare-feu, hyperviseurs, baies de stockage, etc.) ou accès physique aux salles serveurs de l'organisation	La partie prenante met en œuvre une politique de management du risque. La politique est intégrée et se réalise de manière proactive.	Les intentions de la partie prenante sont parfaitement connues et pleinement compatibles avec celles de l'organisation étudiée	4

Le programme de revue est élaboré sur la base de ces critères par le pôle sécurité de la DSN et soumis à validation à la Déléguée à la protection des données, à l'AGEPS et au Directeur de la DSN ou son représentant.

Un bilan annuel des revues est effectué afin d'adapter si besoin la présente procédure.

Afin d'optimiser les ressources, la revue est réalisée au travers d'un questionnaire électronique administré avec le service DASTRA <https://app.dastra.eu/>. Le modèle de questionnaire est joint en annexe de la présente procédure.

Répartition des Rôles dans la gestion des relations avec les Fournisseurs :

- L'AGEPS est responsable de la gestion des relations avec les Fournisseurs sur le plan juridique et administratif y compris les mises en demeure en cas de manquements
- La Déléguée à la protection des données apporte son expertise en matière de protection des données personnelles. Elle contribue à la procédure de revue des fournisseurs
- Le pôle SSI de la DSN apporte son expertise en matière de sécurité de l'information. Il tient à jour le registre des fournisseurs les plus critiques. Il propose annuellement le programme de revue des fournisseurs
- Le pôle Ressources de la DSN assure l'exécution du Marché/Contrat.
- Le pôle de la DSN, qui assure le volume prestation le plus élevé avec un Fournisseur, est désigné comme chef de file. Il est chargé d'organiser et de conduire la revue avec le Fournisseur dans les locaux de l'AP-HP ou à défaut à distance. Il saisit l'AGEPS lorsque des insuffisances sont observées dans les prestations en informant les pôles Ressources et Sécurité de la DSN et la Déléguée à la protection des données
- Le Fournisseur constitue le fonds documentaire nécessaire à la revue. Il le communique au pôle chef de file 7 jours calendaires avant la tenue de la revue. Le Fournisseur produit le compte-rendu de la revue sous 2 jours ouvrés. L'AP-HP dispose de 7 jours pour émettre ses observations et valider le compte-rendu dès qu'il n'y a plus d'observations.

Pour les autres Fournisseurs, une revue est organisée à la fin du Marché ou en cas de changement important dans le volume ou la nature des prestations, de rachat, de changement de pays...

En cas de survenance d'un incident de sécurité d'une gravité supérieure ou égale à 3 (Cf. Matrice Impact-Gravité à la page n°23) ou lors de l'identification d'un risque critique impliquant le Fournisseur, un audit de sécurité du Fournisseur pourra être diligenté par l'AP-HP.

5 EXIGENCES DE SÉCURITÉ

5.1 Protection des données personnelles

Dans le cadre de leurs relations contractuelles, le Fournisseur et l'AP-HP s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 en vigueur (ci-après, « le règlement européen sur la protection des données »), la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée et le Code de la Santé Publique (CSP).

5.1.1 Traitements réalisés par l'AP-HP

Dans le cadre de son activité, l'AP-HP collecte des données à caractère personnel du Fournisseur, qui font l'objet de traitements automatisés dans les conditions prévues par la loi n°78-17 précitée, à des fins (a) de gestion de la relation Fournisseur (facturation, assistance et maintenance des Services, gestion commerciale, archivage, téléphonie, amélioration de la qualité, de la sécurité et de la performance des services, recouvrement, etc.), et (b) de respect de la réglementation applicable à l'AP-HP (notamment obligations légales de conservation des données de connexion et d'identification des utilisateurs).

L'AP-HP s'engage à ne pas utiliser les données ainsi collectées à d'autres fins que celles susmentionnées. L'AP-HP peut toutefois être amenée à devoir les communiquer à des autorités judiciaires et / ou administratives, notamment dans le cadre de réquisitions. En ce cas, et sauf disposition légale l'en empêchant, l'AP-HP s'engage à en informer le Fournisseur et à limiter la communication de données à celles expressément requises par lesdites autorités.

Les données traitées à des fins de gestion de la relation entre le Fournisseur et l'AP-HP sont constituées d'informations telles que NOM, prénom, adresse postale, adresse électronique, numéro téléphone et sont conservées par l'AP-HP pendant toute la durée du Marché/Contrat et les trente-six (36) mois suivants. Les données de connexion et d'identification sont conservées par l'AP-HP pendant douze (12) mois. Les autres données à caractère personnel collectées et traitées par l'AP-HP afin de respecter ses obligations légales, sont conservées conformément à la loi applicable.

Dans le cadre des finalités définies ci-dessus, le Fournisseur accepte que les données à caractère personnel susvisées le concernant soient transférées par l'AP-HP à ses sous-traitants qui interviennent dans le cadre de l'exécution des Marchés/Contrats. Celles-ci ne pourront toutefois accéder à ces données à caractère personnel que dans le cadre des finalités susmentionnées, et dans le strict respect des droits du Fournisseur en matière de protection des données à caractère personnel.

Conformément à la loi « Informatique et Libertés » du 6 janvier 1978 modifiée, le Fournisseur bénéficie d'un droit d'accès, de rectification et de suppression des informations susvisées le concernant. Il peut exercer ce droit et obtenir communication desdites informations auprès du Délégué à la Protection des Données (DPO) de l'AP-HP (Cf. coordonnées en annexe) en justifiant de son identité. Il y sera répondu dans un délai de trente (30) jours suivant réception.

Le Fournisseur dispose également du droit d'introduire une réclamation auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL).

5.2 Confidentialité

Le Fournisseur qui, soit avant la notification du Marché ou la signature du Contrat, soit au cours de son exécution, a reçu communication, à titre confidentiel, de renseignements ou de documents quelconques, est tenu de maintenir confidentielle cette communication.

L'obligation de confidentialité s'étend aux données intéressant les patients et les personnels de l'AP-HP dont le Fournisseur, pourrait avoir connaissance dans le cadre de l'exécution des prestations.

Dans tous les cas, ces renseignements ou documents ne peuvent pas, sans autorisation, être communiqués à d'autres personnes que celles qui ont qualité pour les connaître.

Le Fournisseur se porte fort du respect par ses salariés et sous-traitants et plus généralement de toutes personnes – personnes morales comme personnes physiques - intervenant pour le compte du Fournisseur du principe de confidentialité des données précitées.

Indépendamment de l'éventuel engagement de sa responsabilité pénale, il assumera donc à ce titre, à l'égard de l'AP-HP, toutes conséquences de droit, en cas de divulgation des informations confidentielles par ses salariés, ses sous-traitants et leurs salariés.

Le Fournisseur comme l'AP-HP s'engagent à ne pas divulguer à des tiers les documents, les informations et les renseignements communiqués par l'autre partie à l'occasion de l'exécution du présent Marché, sauf, en cas d'accord écrit donné par l'AP-HP et/ou par le Fournisseur, lorsque les informations sont tombées officiellement dans le domaine public, lorsque les informations sont indiquées par la partie qui les communique à chaque communication, comme n'étant pas confidentielles, lorsque les informations sont diffusées au public préalablement à la notification du Marché ou lorsque les informations sont intégrées dans le produit. Toute communication du Fournisseur vers les tiers, à l'exception des Sociétés Affiliées et sous-traitants du Fournisseur, concernant le Marché et son exécution doit être préalablement soumise à l'accord de l'AP-HP.

Pour Société Affiliées du Fournisseur, on entend toute personne morale, directement ou indirectement contrôlant, contrôlée par ou placée sous contrôle commun avec le Fournisseur. Aux fins de la présente définition, la notion de « contrôle » est celle indiquée à l'article L 233-3 du Code de commerce.

Le Fournisseur veille à ce qu'au cours de l'exécution du Marché, soient respectées la sécurité et la confidentialité des Données et des accès informatiques, de l'AP-HP conformément aux lois et régimes applicables, et notamment la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, les dispositions du Code de la propriété intellectuelle applicables aux logiciels et bases de données et celles du Code pénal. Par ailleurs, le Fournisseur s'engage à ne pas conduire l'AP-HP à méconnaître ces dispositions, en procédant à toutes les préconisations utiles en ce sens.

Le Fournisseur s'engage par ailleurs à ne prendre aucune copie des supports, ne pas utiliser les documents à des fins autres que celles spécifiées dans le Marché, ne pas utiliser ou diffuser, sans autorisation préalable écrite de l'AP-HP, à l'exception des Sociétés Affiliées et sous-traitants du Fournisseur, aucune partie ou totalité d'un programme, d'un fichier et/ou d'une donnée détenu(s) par l'AP-HP ou installé(s) sur un élément ou sur un sous-ensemble d'une configuration, d'un matériel ou d'une pièce détachée détenu(s) par l'AP-HP, et/ou aucune documentation détenue par l'AP-HP, à prendre toute mesure, notamment de sécurité matérielle pour assurer la conservation des supports tout au long de la durée du Marché.

Le non-respect de ces dispositions expose le Fournisseur à l'application des mesures prévues à l'article « Résiliation » du CCAP du Marché.

5.3 Sécurité

Le Fournisseur et ses sous-traitants ultérieurs sont tenus de respecter :

- La charte du bon usage du système d'information de l'AP-HP annexe n°16 du règlement intérieur de l'AP-HP

- Les prescriptions de la politique générale de sécurité des systèmes d'information (PGSSI) de l'AP-HP annexée au présent Marché ainsi que les directives, les procédures et modes opératoires pris en application de la PGSSI.

Les directives, les procédures et modes opératoires sont communiqués au Fournisseur sur demande motivée par voie électronique dans un délai de 15 jours ouvrés.

Dans tous les cas, le Fournisseur est tenu de fournir à la première demande la documentation nécessaire à la sécurisation de ses prestations et fournitures, la protection des données des bénéficiaires et aux démonstrations du respect de ses obligations.

5.3.1 Accès à la documentation et aux informations par le Fournisseur

L'AP-HP communique au Fournisseur les types d'information et documents auxquelles le Fournisseur pourra accéder dans le cadre de ses prestations.

Par défaut, l'accès aux autres catégories d'information et documents est interdit.

Conformément à la charte du bon usage du système d'information de l'AP-HP annexe n°16 du règlement intérieur de l'AP-HP, l'AP-HP met en œuvre des dispositifs d'identification et d'authentification, de contrôle d'accès, et traçabilité pour assurer la sécurité des informations. Le Fournisseur reconnaît être informé que de tels dispositifs sont mis en place. Le Fournisseur et ses sous-traitants ultérieurs informent leurs personnels de la mise en œuvre de ces dispositifs par l'AP-HP. L'AP-HP s'engage à respecter la législation en la matière.

5.3.2 Signalements de failles ou d'incidents de sécurité

Le Fournisseur informe l'AP-HP sous un délai de 72 heures au plus, de la découverte de faille(s) de sécurité ou d'un incident de sécurité impactant l'exécution des prestations. L'adresse de messagerie aphp-signalement-securite@aphp.fr est utilisé pour ce faire.

Toute faille ou incident de sécurité jugé comme significatif par l'AP-HP est obligatoirement notifié aux autorités compétentes (ANS, ANSSI, CNIL...) par l'AP-HP.

Le Fournisseur a obligation d'enregistrer les failles auprès des autorités compétentes, le CERT-FR pour la France, en suivant les réglementations établies. A défaut d'action sous 3 mois, l'AP-HP a la possibilité de se substituer au Fournisseur dans les actions précédentes et de pratiquer une divulgation responsable (annonce de la faille avec embargo pendant au moins 90 jours sur les détails techniques).

5.3.3 Protection contre les logiciels malveillants

Le Fournisseur doit protéger les systèmes d'information utilisés pour la réalisation des Prestations conformément à l'état de l'art en matière d'hygiène informatique et de sécurité, notamment avec des logiciels à jour, un anti-virus activé actualisé au moins toutes les 12 heures.

5.3.4 Gestion des vulnérabilités techniques

Le Fournisseur est tenu de réaliser une gestion des vulnérabilités des systèmes et logiciels qu'il met en œuvre dans le cadre de sa Prestation. Il s'engage à apporter les corrections nécessaires dans des délais raisonnables au vue de la criticité des vulnérabilités et du niveau d'exposition aux menaces. Le Fournisseur informera régulièrement de l'état de l'application des correctifs de sécurité. Toute vulnérabilité pouvant avoir un impact sur la sécurité de l'AP-HP sera notifié au RSSI de l'AP-HP.

5.3.5 Echanges et communications d'informations

L'usage de la messagerie entre le Fournisseur et l'AP-HP se limite à des échanges non confidentiels.

Le Fournisseur et l'AP-HP s'engagent à utiliser la plateforme d'échange de fichiers <https://dispose.aphp.fr> conformément aux conditions générales d'utilisation du service lors de la transmission d'informations sensibles et s'interdit de les communiquer par tout autre moyen sauf impossibilité technique.

Le Fournisseur et l'AP-HP s'engagent à limiter l'usage des supports amovibles et à privilégier la plateforme d'échange de fichiers <https://dispose.aphp.fr>.

5.3.6 Accès physiques aux locaux de l'AP-HP

L'AP-HP assure au personnel du Fournisseur appelé à intervenir dans ses locaux, des conditions d'environnement conformes aux normes d'hygiène et de sécurité.

L'AP-HP informe le Fournisseur des consignes de sécurité dans lesdits locaux et emprises.

L'accès aux locaux de l'AP-HP par le Fournisseur est soumis au règlement intérieur (RI) de l'AP-HP.

L'AP-HP tient à jour un registre nominatif des personnels du Fournisseur, autorisés à intervenir dans ses locaux. Seuls les personnels du Fournisseur régulièrement inscrites aux registres peuvent avoir accès aux clés, badges permanents, codes, matériels ou locaux utilisés pour assurer la protection physique des informations et ressources informatiques appartenant à l'AP-HP. Ils s'engagent à les garder secrets, à ne pas les dévoiler ou les laisser à la disposition des tiers, à informer sans délai l'AP-HP en cas de perte ou de vol.

Au cours de ses visites dans les locaux de l'AP-HP, le personnel du Fournisseur ne peut être accompagné d'un tiers sans accord écrit préalable de Personne Publique ou du responsable du site concerné.

Aucune sortie des locaux de l'AP-HP de configurations, de supports numériques ou autres, d'éléments ou sous-ensembles de configuration, de matériel, de pièce détachée et/ou de documentation détenus par l'AP-HP ne peut être faite sans l'autorisation préalable et écrite de l'AP-HP.

Dans le cas des opérations de maintenance (par exemple, réparation matérielle), le Fournisseur doit transmettre au préalable à l'AP-HP un descriptif précisant les dates, la nature des opérations à effectuer et les noms des intervenants.

L'AP-HP veille à la présence effective de l'un de ses personnels qualifiés pendant la durée de l'intervention dudit personnel, de telle sorte que toutes mesures utiles puissent être immédiatement prises en cas d'accident.

Dans le cas de la livraison d'une solution ou de matériel (par exemple : stock informatique, papiers, mobilier), il est toléré que l'accès du bâtiment soit provisoirement ouvert le temps des opérations de livraison. Le personnel de l'AP-HP, à défaut du Fournisseur, est chargé de veiller à surveillance des accès et à la fermeture systématique des accès et des locaux dès la livraison terminée.

Les personnels du Fournisseur s'engagent à :

- Respecter les directives et procédures de sécurité de l'AP-HP
- Informer sans délai l'AP-HP de tout départ, changement de fonction de ses personnels
- A ne pas tenter de contourner les procédures mises en œuvre par l'AP-HP permettant le contrôle des accès autorisés et empêchant les accès non autorisés à ses locaux
- Ne pas essayer de s'introduire dans des locaux non autorisés ou avec d'autres moyens que ceux mis à sa disposition
- Ne pas permettre l'accès aux personnes non autorisées par l'AP-HP dans ses locaux
- Respecter les systèmes de sécurité physique mis en place à l'AP-HP, en particulier fermer systématiquement à clé s'il le peut, les portes derrière lui, même en cas d'absence de courte durée
- Assurer la protection physique du matériel mis à sa disposition
- Restituer tous les objets mis à disposition l'AP-HP permettant l'accès physique aux locaux de l'AP-HP infrastructures à la fin de l'intervention
- Ne réaliser aucune copie ou duplicata des moyens d'accès mis à disposition
- Ne pas entraver le fonctionnement des équipements opérationnels et ceux de sécurité
- Signaler tout défaut de sécurité ou situation qui semblerait anormale.

5.3.7 Vidéo protection

Afin d'assurer la sécurité des biens ou des personnes, certains sites ou lieux sensibles de l'AP-HP ont été équipés de système de vidéo protection. Le Fournisseur reconnaît être informé que de tels systèmes sont mis en place dans les sites et locaux sensibles. Le Fournisseur et ses sous-traitants ultérieurs informent leurs personnels de la mise en œuvre de ces traitements par l'AP-HP. L'AP-HP s'engage à respecter la législation applicable à ce type d'équipement notamment l'affichage obligatoire.

5.3.8 Connexion du matériel du Fournisseur sur les réseaux de l'AP-HP

Dans le cas où le Fournisseur aurait besoin, pour l'exécution de ses prestations, de connecter des matériels informatiques lui appartenant sur le réseau de l'AP-HP, le Fournisseur s'engage à :

- Recueillir préalablement l'accord express de l'AP-HP
- Respecter la charte du bon usage du système d'information de l'AP-HP annexe n°16 du règlement intérieur de l'AP-HP, les directives de sécurité et procédures de l'AP-HP
- Ne pas entraver ou de contourner la mise en œuvre et l'action des dispositifs de sécurité de l'AP-HP.
- Garantir que son matériel ne présente aucun risque de compromission ou d'infection par un code informatique malveillant, du réseau informatique de l'AP-HP notamment par une analyse préalable avec un antivirus à jour avant chaque connexion au système d'information de l'AP-HP
- Garantir que cette connexion n'a en aucune manière un impact sur les performances, la disponibilité, l'intégrité et la confidentialité du Système d'Information de Personne Publique
- Chiffrer les données au repos avec un dispositif à l'état de l'art
- Pour les dispositifs ayant une capacité autonome de traitement de l'information (téléphone multifonction, poste de travail informatique...) :
Garantir la présence d'un antivirus à jour et à même de récupérer au moins 1 fois toutes les 24h les dernières signatures antivirales
Utiliser un système d'exploitation dans une version maintenue et à jour des correctifs de sécurité et à même de récupérer et d'installer au moins 1 fois par semaine les derniers correctifs de sécurité
Respecter les contraintes d'adressage MAC/IP
Utiliser des protocoles de communication sans faille connue

Pour les actes d'administration ou d'exploitation qui seraient réalisés par le Fournisseur, le Fournisseur utilise des postes de travail informatiques dédiées à l'exploitation et l'administration isolées des réseaux bureautiques, d'Internet, de la messagerie notamment. Si ces actes sont réalisés depuis les locaux de l'AP-HP, les postes de travail informatiques sont fournis par l'AP-HP.

5.3.9 Accès au système d'information de l'AP-HP par le Fournisseur

Dans le cas où le Fournisseur aurait besoin, pour l'exécution de ses prestations, d'accéder au système d'information de l'AP-HP, le Fournisseur s'engage à :

- Recueillir préalablement l'accord express de l'AP-HP
Tout professionnel du Fournisseur accédant au SI de l'AP-HP doit impérativement recevoir et signer un engagement individuel de confidentialité
- Respecter la charte du bon usage du système d'information de l'AP-HP annexe n°16 du règlement intérieur de l'AP-HP, les directives de sécurité et procédures de l'AP-HP
- Identifier nommément ses personnels, en communiquer la liste à l'AP-HP et tenir à jour un registre revu au moins annuellement
Chaque compte permettant d'accéder au SI de l'AP-HP est strictement nominatif et n'appartient qu'à un seul prestataire.
S'interdit de réattribuer L'identifiant de connexion à un autre professionnel pour quelque motif que ce soit.
- Informer sans délai l'AP-HP de tout départ, changement de fonction de ses personnels

- A ne pas tenter d'entraver ou de contourner les procédures mises en œuvre par l'AP-HP permettant le contrôle des accès autorisés et empêchant les accès non autorisés à son système d'information
- Traiter les moyens d'authentification comme des informations confidentielles
Le Fournisseur est responsable de la gestion et de la confidentialité de ses moyens d'authentification, nécessaires accéder au système d'information de l'AP-HP. Le Fournisseur s'assure notamment que ses personnels ont connaissance et respectent les règles de l'art permettant de préserver la confidentialité de leurs moyens d'authentification.
Le Fournisseur supporte seul les conséquences pouvant résulter de la perte, la divulgation, ou l'utilisation frauduleuse ou illicite des moyens d'authentification fournis à ses personnels, la responsabilité de l'AP-HP ne pouvant en aucun cas être engagée à ce titre.
- Signaler tout défaut de sécurité ou situation qui semblerait anormale.

Le Fournisseur s'engage à informer l'AP-HP sans délai, de toute perte ou divulgation éventuelle des moyens d'authentification, et à procéder immédiatement au renouvellement desdits moyens d'authentification.

Pour les Services relevant de l'Article L1111-8 du code de la santé publique et afin de garantir la confidentialité des données de santé à caractère personnel et leur protection, l'AP-HP met à disposition du Fournisseur des moyens d'authentification conformes aux référentiels d'interopérabilité et de sécurité élaborés par le groupement d'intérêt public mentionné à l'article L. 1111-24 du code de la santé publique.

5.3.10 Interconnexion entre le SI du Fournisseur et le SI de l'AP-HP

Toute interconnexion avec le SI de l'AP-HP doit être préalablement validée par un écrit de l'AP-HP.

Cette validation inclut un Dossier d'Architecture Technique, comprenant une matrice de flux, la personne à contacter pour tout événement de sécurité et les exigences de sécurité applicables à cette interconnexion.

5.3.11 Télémaintenance/Téléassistance

Dans le cas où le Fournisseur réalise une prestation de maintenance à distance sur des ressources de l'AP-HP ou sur des ressources du Fournisseur, installées sur le réseau de l'AP-HP, le Fournisseur s'engage à respecter les règles suivantes :

- Utiliser le service d'accès à distance mis en œuvre par l'AP-HP dénommé BASTION d'administration WALLIX.
Dans le cas, où le besoin d'accès à distance ne serait pas compatible techniquement avec le service de BASTION d'administration WALLIX, le fournisseur peut demander une dérogation qui sera instruite par l'AP-HP. Dans tous les cas, la solution proposée par le Fournisseur doit, sous peine de non-conformité, garantir que tout accès au système d'information (SI) est nominatif et personnel, mettre en œuvre une authentification forte (par exemple, à deux facteurs) et assurer la traçabilité et journalisation des connexions et des opérations effectuées. L'AP-HP doit pouvoir accéder aux traces et journaux générés.
L'AP-HP se réserve le droit de facturer au Fournisseur les coûts liés à l'instruction de cette dérogation ainsi qu'à sa mise en œuvre technique. Ces coûts incluent, sans s'y limiter : l'analyse et validation de la demande, la mise en œuvre technique et configuration et, le contrôle et suivi. Les frais correspondants seront définis sur la base d'un forfait établi en fonction des travaux réalisés et des ressources mobilisées. Un devis détaillé sera transmis au fournisseur avant toute intervention, et l'exécution des travaux sera conditionnée à l'acceptation écrite de celui-ci. En l'absence d'accord préalable sur les frais associés, l'AP-HP se réserve le droit de refuser la mise en œuvre de la dérogation et d'exiger l'utilisation du bastion d'administration WALLIX comme solution de référence.
- Obtenir l'accord préalable de l'AP-HP avant chaque intervention
- Respecter les directives et procédures de sécurité de l'AP-HP

- A ne pas tenter de contourner les procédures mises en œuvre par l'AP-HP permettant le contrôle des accès autorisés et empêchant les accès non autorisés à son système d'information
- Signaler tout défaut de sécurité ou situation qui semblerait anormale.
- Transmettre systématiquement à l'AP-HP un rapport d'intervention retraçant les opérations menées, les données à caractère personnel accédées, les modifications réalisées sur l'environnement de production et leurs impacts éventuels, et ce quels que soient les composants modifiés (système, applications, middlewares, réseaux...)
- Garantir que son matériel ne présente aucun risque de compromission ou d'infection par un code informatique malveillant, du réseau informatique de l'AP-HP
- Traiter les moyens d'authentification comme des informations confidentielles
- Télé-assister les utilisateurs ou les personnels de l'AP-HP chargés de la mise en œuvre du système d'information conformément aux recommandations de la commission nationale de l'informatique et des libertés (CNIL).

L'AP-HP met gracieusement à disposition du Fournisseur un service de télémaintenance respectant le palier 1 du niveau exigibilité du guide ANS « Règles pour les interventions à distance sur les systèmes d'information de santé - Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) - Décembre 2014 - V1.0 ». Le service comporte une authentification nominative et personnelle ainsi qu'une traçabilité nominative détaillée. Le Fournisseur s'engage à informer ses préposés de la mise en œuvre d'un tel dispositif.

Le Fournisseur peut proposer dans le cadre de ses prestations un dispositif de télémaintenance équivalant respectant le palier 1 du niveau exigibilité du guide ANS « Règles pour les interventions à distance sur les systèmes d'information de santé - Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) - Décembre 2014 - V1.0 ». Après une revue de conformité et en cas de non-conformité ou de difficultés techniques importantes dans la mise en œuvre, l'AP-HP peut refuser la mise en œuvre du dispositif de télémaintenance proposé par le Fournisseur et imposer son service de télémaintenance.

5.3.12 Prestation d'externalisation d'une composante du système d'information de l'AP-HP

Le Fournisseur fournira à l'AP-HP la description de l'ensemble des dispositions qu'il s'engage à appliquer en matière de sécurité pour l'exécution du Marché dans un Plan d'Assurance Sécurité (PAS).

Ce PAS présentera notamment la manière dont le Fournisseur répond opérationnellement aux exigences de sécurité du Marché.

Un modèle de plan de PAS est annexé au présent document.

5.3.13 Homologation de sécurité

L'AP-HP met en œuvre une démarche d'intégration de la sécurité dans les projets et procède à une homologation de sécurité conformément au Référentiel Général de Sécurité (RGS).

Le Fournisseur en charge d'un système nécessitant une homologation de sécurité s'engage à communiquer les éléments requis pour instruire l'homologation à l'AP-HP, à appliquer les exigences validées pour l'homologation, à faire évoluer la documentation lors de tout changement du système et à informer l'AP-HP de tout changement significatif pouvant remettre en cause l'homologation.

5.3.14 Certification hébergeur de données de santé de l'AP-HP

Le Fournisseur atteste avoir pris connaissance de la possible intégration de ses prestations dans le périmètre des prestations rendues par l'AP-HP à ses clients et Partenaire relevant de la certification à l'hébergement de données de santé au cours de l'exécution du Marché/Contrat en application de l'Arrêté du 11 juin 2018 portant approbation du référentiel d'accréditation des organismes de certification et du référentiel de certification pour l'hébergement de données de santé à caractère personnel.

L'AP-HP informe le Fournisseur de cette intégration lors de la phase de consultation.

Le Fournisseur s'engage à ne pas faire obstacle à la mise en œuvre des mesures de sécurité prescrite par le référentiel de certification HDS - Exigences et contrôles - Version 1.1 finale – Mai 2018.

Le Fournisseur informe l'AP-HP des conséquences sur l'exécution de ses prestations.

Le Fournisseur et l'AP-HP peuvent convenir d'un avenant au Marché/Contrat afin d'adapter les conditions d'exécution des prestations s'il n'a pas été possible d'informer le Fournisseur lors de de la phase de consultation.

5.3.15 Système d'information essentiel de l'AP-HP

Le Fournisseur atteste avoir pris connaissance de la possible intégration de ses prestations dans le périmètre des prestations rendues par l'AP-HP à ses clients et Partenaire relevant de la directive européenne Network and Information System Security (NIS) et à la loi n°2018-133 du 26 février 2018 de transposition de la directive en droit français.

L'AP-HP informe le Fournisseur de cette intégration lors de la phase de consultation.

Le Fournisseur s'engage à ne pas faire obstacle à la mise en œuvre des mesures de sécurité prescrite par l'Arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'article 10 du décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique

Le Fournisseur informe l'AP-HP des conséquences sur l'exécution de ses prestations.

Le Fournisseur et l'AP-HP peuvent convenir d'un avenant au Marché/Contrat afin d'adapter les conditions d'exécution des prestations s'il n'a pas été possible d'informer le Fournisseur lors de de la phase de consultation.

5.3.16 Certification hébergeur de données de santé du Fournisseur

Le Fournisseur s'engage à être certifié hébergeur de données de santé pour la durée du Marché/Contrat sur le périmètre des prestations traitant des données de santé relevant de la certification conformément aux règles édictées par l'Agence du Numérique en Santé (ANS).

Le Fournisseur met à disposition de l'AP-HP le certificat et le rapport d'audit de certification initial ainsi qu'annuellement chaque rapport d'audit de suivi.

Le Fournisseur informera l'AP-HP de tout risque de perte de cette certification.

5.4 Les exigences fonctionnelles de sécurité

Le présent ensemble de clauses s'applique aux Marchés/Contrats concernant les prestations de :

- Fourniture de logiciels commerciaux
- Etudes et de mise au point de logiciels spécifiquement conçus et produits pour répondre aux besoins particuliers
- Elaboration de systèmes d'information
- Tierce maintenance applicative.

Le présent ensemble de clauses ne s'applique pas

- Fourniture de matériel informatique ou de télécommunication
- Fourniture de logiciels bureautiques
- Prestations de maintenance ou d'infogérance.

5.4.1 Identification/Authentification

La composante privée du Système accédée doit identifier et authentifier de façon unique les utilisateurs [l'utilisation de comptes partagés n'est pas autorisée]. Il peut exister une composante publique [consultation de données par exemple] ne nécessitant pas d'authentification préalable.

Lorsqu'elles sont nécessaires, l'identification et l'authentification doivent avoir lieu avant toute autre interaction entre la ressource accédée et l'utilisateur. D'autres interactions ne doivent être possibles qu'après une identification et une authentification réussie.

Lorsqu'elles sont nécessaires, l'identification et l'authentification avec l'utilisateur doivent être réalisées au sein d'un environnement sûr. Pour chaque interaction, le Système doit pouvoir établir l'identité de l'utilisateur.

Dans le cas où l'authentification est déportée vers un frontal d'authentification, un chemin sûr [dit de confiance] doit être établi entre le frontal et le Système. La confiance dans ce chemin pourra être atteinte par la mise en place de solutions techniques, procédurales ou organisationnelles. L'utilisation d'un tel frontal ne nuira pas à la mise en place des fonctions de journalisation et d'audit (cf. ci-après).

Lorsque les techniques d'authentification mettent en œuvre des mécanismes cryptographiques, ceux-ci devront présenter un niveau de robustesse au moins équivalent au niveau de robustesse standard défini par l'ANSSI et le Référentiel général de Sécurité (RGS).

Si des moyens d'authentification par mot de passe sont mis en œuvre, le Système doit permettre de contrôler la mise en œuvre d'une politique de gestion rigoureuse : durée de validité du secret, taille minimale et format, gestion des renouvellements et des secrets passés, gestion du nombre de tentatives infructueuses.

Des moyens cryptographiques doivent être mis en œuvre pour garantir la confidentialité et l'intégrité des données d'authentification en transit ou stockées. Ces moyens doivent être cohérents avec la durée de validité retenue pour les paramètres d'authentification et présenter un niveau de robustesse au moins équivalent au niveau de robustesse standard défini par l'ANSSI et le RGS.

Des mesures doivent être mises en œuvre pour garantir l'intégrité des mécanismes d'authentification.

Le Système doit mettre en œuvre une authentification SAML2 ou OPENID CONNECT. L'AP-HP met à disposition du Fournisseur un IDP. Cet IDP utilise une méthode d'authentification par LOGIN/Mot de passe quand l'accès se fait depuis le réseau de l'AP-HP, complété par une authentification à 2 facteurs pour les accès depuis Internet (cas du télétravail).

Si le système traite de données de santé, les moyens d'identification et d'authentification sont conforme au référentiel d'identification électronique des usagers, des acteurs des secteurs sanitaire-médico-social-et-social pour les personnes morales ou physiques de l'ANS.

5.4.2 Contrôle d'accès

Le Système doit pouvoir distinguer et administrer les droits d'accès de chaque utilisateur [au niveau d'un utilisateur individuel, au niveau de l'appartenance à un groupe d'utilisateurs, ou aux deux niveaux].

Il doit être possible de refuser complètement à des utilisateurs ou à des groupes d'utilisateurs l'accès à un répertoire, un fichier ou une fonction du Progiciel.

Il ne doit pas être possible à quelqu'un qui n'est pas un utilisateur autorisé d'accorder ou de retirer des droits d'accès au sein du Système.

Il doit également être possible de limiter l'accès en lecture seulement selon les besoins.

Il doit être possible d'accorder les droits d'accès à un objet (répertoire, fichier, fonction) en descendant jusqu'au niveau de granularité de l'utilisateur individuel.

L'administration des droits doit disposer de contrôles pour limiter la propagation des droits d'accès. Seuls des utilisateurs autorisés doivent pouvoir créer de nouveaux comptes utilisateurs, supprimer ou désactiver des comptes utilisateurs existants.

Lors de toute tentative par des utilisateurs ou des groupes d'utilisateurs d'accéder à un répertoire, un fichier, ou une fonction du Système, le Système doit vérifier la validité de la demande. Les tentatives d'accès non autorisés doivent être rejetées.

5.4.3 Journalisation / imputabilité

Le Système doit comporter un composant d'imputation qui soit capable de journaliser :

Les tentatives d'identification et d'authentification [données exigées : date, heure, identité fournie par l'utilisateur, identification de l'équipement sur lequel le mécanisme d'identification et d'authentification a été utilisé, réussite ou échec de la tentative, autorisation de l'utilisateur].

Les actions d'administration [données exigées : Date, heure, identité de l'utilisateur, type de l'action].

En complément, le Système doit pouvoir journaliser certains événements identifiés comme sensibles par les maîtrises d'ouvrage. Les accès à des fichiers, répertoires ou fonctions présentant un caractère sensible [données exigées : Date, heure, identité de l'utilisateur, fonction mise en œuvre, identification de l'objet accédé, type de tentative d'accès, réussite ou échec de la tentative].

Il doit être possible de mettre sélectivement en œuvre l'imputation pour un ou plusieurs utilisateurs.

Les données journalisées ne doivent être accessibles qu'en consultation aux seuls utilisateurs autorisés. Elles doivent être protégées contre tout type de modification ou suppression, afin de garantir l'imputabilité de l'utilisation du Système. Toute action sur une donnée d'imputation devra être tracée

5.4.4 Audit

Il doit exister des outils pour examiner les fichiers d'imputation pour les besoins d'audit et ces outils doivent être documentés. Ils doivent permettre d'identifier sélectivement les actions d'un ou de plusieurs utilisateurs.

5.4.5 Protection de l'intégrité du Système

En standard, l'intégrité du Système est assurée par les moyens de contrôle d'intégrité des bases de données et des serveurs mis en place systématiquement par l'AP-HP.

Toute donnée envoyée ou reçue en pièce jointe doit être identifiée et contrôlée. Des précautions doivent être prises afin de prévenir et détecter l'introduction de tout code malveillant par l'intermédiaire des informations transmises, ou pour prévenir toute saturation du Système par l'envoi de pièces de taille anormalement volumineuse. Le contrôle du type et format des données entrantes et sortantes sera assuré par des dispositifs de protection permettant l'analyse de code malveillant, l'analyse de requête autorisée, l'analyse de type et format de données échangées.

5.5 Méthodologie sécurisée d'ingénierie et de développement

Le Fournisseur met en œuvre une méthodologie d'ingénierie et de développement sécurisée pour son Système. Le Fournisseur décrit ses activités et contrôles de sécurité, utilisés en la matière (processus, procédures, outillages, indicateurs). Il s'agit notamment de :

- Formation en lien avec la sécurité des développements
- Définition des exigences de sécurité
- Modélisation de la menace
- Usage d'outils évalués et approuvés
- Gestion des risques de sécurité relatifs à l'usage des logiciels tiers
- Définition des exigences de conception
- Analyse statique et dynamique du code
- Test d'intrusion
- Processus standard de réponse aux défauts et incidents

- Indicateur de pilotage des activités en lien avec la sécurité de l'information
- Rapport de conformité.

Le Fournisseur assurant une prestation de développement s'engage à respecter les bonnes pratiques de sécurité dans le développement, en sus de respecter les exigences de sécurité exprimées dans la documentation sur la sécurité de l'information de l'AP-HP.

5.6 Gestion des évolutions

Les évolutions fonctionnelles ou techniques ne doivent pas remettre en cause le respect des exigences de sécurité ou compromettre les éventuelles opérations de réversibilité. En cas d'évolution, le Fournisseur devra vérifier que sa mise en œuvre est conforme aux exigences contractuelles et en apporter la justification auprès de l'AP-HP, avant validation par ce dernier.

5.7 Audits

5.7.1 Audit par le Fournisseur

Agrément relatif à l'auditeur

L'auditeur proposé par le Fournisseur doit être agréé par l'AP-HP. Aucun auditeur ne peut être imposé à l'AP-HP, dans la mesure où il peut présenter un risque de partialité. Il doit être reconnu en tant qu'auditeur indépendant, c'est-à-dire indépendant du Fournisseur, ayant une qualification adéquate, et libre de fournir les détails de ses remarques et conclusion d'audit à l'AP-HP.

Agrément relatif à l'audit

La réalisation de l'audit du Fournisseur est soumise à l'agrément de l'AP-HP. Afin de permettre à l'AP-HP de procéder à l'agrément de l'audit, le Fournisseur fournit à l'AP-HP une lettre de cadrage de l'audit par « lettre recommandée avec avis de réception postale » (ou équivalent) mentionnant notamment : le périmètre des investigations, les limitations, les moyens techniques mis en œuvre, la date proposée, la durée, et toutes informations jugées utiles. Ce document retrace donc notamment l'ensemble des moyens techniques, outils, méthodes... qui sont mis en œuvre lors de l'audit.

L'agrément ne pourra être délivré que dans la mesure où :

- L'audit du Fournisseur ne suscite pas d'impact sur la production de l'AP-HP ni sur le bon fonctionnement de ses services et services associés
- Le Fournisseur respecte un délai de prévenance de deux (2) mois pour soumettre l'agrément de l'audit et de l'auditeur à l'AP-HP.

Modalités complémentaires de délivrance de l'agrément

A réception de l'ensemble des éléments nécessaires pour engager la procédure d'agrément, l'AP-HP dispose d'un (1) mois pour se prononcer sur l'agrément ou le rejet de la demande d'audit.

Modalités liées à la réalisation de l'audit

Le Fournisseur prend en charge l'intégralité des coûts de l'audit, dont notamment la rémunération de l'auditeur interne ou externe, la prise en charge des coûts liés à la mobilisation de ressources humaines internes aux taux horaires desdites personnes...

La personne Publique se réserve la faculté de modifier la date prévue de l'audit :

- Dans la limite de deux (2) reports par demande d'audit
- Avec report de la date de l'audit dans un délai maximal d'un (1) mois suivant la date prévisionnelle agréée.

Responsabilité liée à l'audit

Le Fournisseur engage son entière responsabilité au titre des préjudices qui pourraient naître au détriment de l'AP-HP à l'occasion de l'audit et qui résulteraient, notamment, d'une faute, erreur ou omission de l'auditeur.

Confidentialité liée aux résultats de l'audit

Le Fournisseur s'engage à respecter la plus stricte confidentialité au titre des éléments qu'il serait amené à connaître dans le cadre de l'audit. Il s'engage notamment à ne pas divulguer les résultats de l'audit réalisé à des tiers de l'accord concerné par l'audit.

5.7.2 Audit par l'AP-HP

Sous réserve d'un préavis de dix (10) jours ouvrés, l'AP-HP se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect par le Fournisseur de ses obligations au titre du Marché/Contrat, notamment par le biais d'un audit.

Le Fournisseur s'engage à répondre aux demandes d'audit de l'AP-HP et effectuées par l'AP-HP elle-même ou par un tiers de confiance qu'elle aura sélectionné, reconnu en tant qu'auditeur indépendant, c'est-à-dire indépendant du Fournisseur, ayant une qualification adéquate, et libre de fournir les détails de ses remarques et conclusion d'audit à l'AP-HP.

Les audits doivent permettre une analyse du respect des obligations contractuelles, réglementaires et légales, notamment : par la vérification de l'ensemble des mesures de sécurité mises en œuvre par le Fournisseur, par la vérification des journaux de localisation des données, de copie et de suppression des données, par l'analyse des mesures mises en place pour supprimer les données, pour prévenir toutes transmissions illégales de données à des juridictions non adéquates ou pour empêcher le transfert de données vers un pays non autorisé. L'audit doit enfin pouvoir permettre de s'assurer que les mesures de sécurité et de confidentialité mises en place ne peuvent être contournées sans que cela ne soit détecté et notifié.

Il est toutefois entendu qu'un tel audit ou toute autre forme de contrôle/vérification ne peut en aucun cas porter sur les documents financiers et/ou comptables du Fournisseur ou sur les documents relatifs aux membres du personnel du Fournisseur (sauf accord préalable et éclairé de ces derniers). L'AP-HP s'engage à respecter les obligations de confidentialité qui lui incombent au titre des présentes ainsi que les règles d'accès et de sécurité en vigueur dans les locaux du Fournisseur et se porte fort du respect de ces règles par les membres de son personnel et/ou auditeur externe.

6 ANNEXES

Définitions

Les définitions de l'Article 4 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données s'appliquent aux termes suivants :

« données à caractère personnel », « traitement », « limitation du traitement », « profilage », « pseudonymisation », « fichier », « responsable du traitement », « sous-traitant », « destinataire », « tiers », « consentement », « violation de données à caractère personnel », « données génétiques », « données biométriques », « données concernant la santé », « établissement principal », « représentant », « entreprise », « groupe d'entreprises », « règles d'entreprise contraignantes », « autorité de contrôle », « autorité de contrôle concernée », « traitement transfrontalier », « objection pertinente et motivée », « service de la société de l'information » et « organisation internationale » lorsqu'ils sont cités dans tous les documents et enregistrements.

Les définitions de la norme NF ISO/CEI 27000 FÉVRIER 2011 s'appliquent aux termes suivants :

« acceptation des risques », « actif », « actif informationnel », « action corrective », « action préventive », « analyse des risques », « appréciation des risques », « attaque », « authentification », « confidentialité », « continuité de l'activité », « contrôle d'accès », « critères de risque », « disponibilité », « enregistrement », « estimation des risques », « évaluation des risques », « événement lié à la sécurité de l'information », « fiabilité », « gestion des incidents liés à la sécurité de l'information », « gestion du risque », « incident lié à la sécurité de l'information », « impact », « intégrité », « menace », « mesure de sécurité », « non-répudiation », « objectif de sécurité », « politique », « procédure », « processus », « risque », « risque lié à la sécurité de l'information », « sécurité de l'information », « système de management », « système de management de la sécurité de l'information », « traitement des risques » et « vulnérabilité » lorsqu'ils sont cités dans tous les documents et enregistrement.

Checklist

Cette checklist permet à l'AP-HP d'identifier le contexte d'intervention du Fournisseur.

Elle facilite l'identification par le Fournisseur de ses obligations. Le Fournisseur joint la checklist complétée à son offre.

Dans le cadre de l'exécution de ses obligations contractuelles à l'égard de l'AP-HP, le Fournisseur

1. A la qualité de : ☐ Sous-traitant, ☐ Responsable de traitement, ☐ Co-responsable de traitement
2. Traite des données : ☐ Personnelles, ☐ Personnelles de Santé, ☐ Personnelles sensibles autres
3. Accède aux : ☐ locaux, ☐ locaux sensibles, ☐ locaux informatiques
4. Accède aux : ☐ zones sous vidéo protection, ☐ locaux sous vidéo protection
5. Connecte du matériel sur les réseaux de l'AP-HP : ☐ OUI, ☐ NON
6. Accède au système d'information de l'AP-HP : ☐ OUI, ☐ NON
7. Interconnecte son SI avec le SI de l'AP-HP : ☐ OUI, ☐ NON
8. Réalise des prestations de Télémaintenance/Téléassistance : ☐ OUI, ☐ NON
9. Héberge une composante du SI de l'AP-HP : ☐ OUI, ☐ NON
10. Contribue aux homologations de sécurité : ☐ OUI, ☐ NON
11. Intervient sur le périmètre du SI certifié HDS/ISO 27001 de l'AP-HP : ☐ OUI, ☐ NON
12. Intervient sur un Système d'Information Essentiel (SIE) de l'AP-HP : ☐ OUI, ☐ NON

Coordonnées

Délégation à la protection des données

Téléphone : +33 1 40 27 30 00

Courriel à l'adresse électronique : protection.donnees.dsi@aphp.fr

Courrier postal à l'adresse : AP-HP, Délégue à la protection des données – Direction des Services

Numériques - 33, Bd de Picpus, CS 21705, 75571 Paris Cedex 12

Responsable de la sécurité du système d'information

Téléphone : +33 1 40 27 30 00

Courriel à l'adresse électronique : aphp-signalement-securite@aphp.fr

Courrier postal à l'adresse : AP-HP, RSSI – Direction des Services Numériques - 33, Bd de Picpus, CS 21705, 75571 Paris Cedex 12

Matrice Impact-Gravité

Impact sur les personnes concernées					
Echelle de gravité	1	2	3	4	5
Prise en charge	Prise en charge inchangée	Escalade de la surveillance ou du traitement	Menace vitale	Incapacité	Décès
Continuité de l'hospitalisation	Pas de discontinuité	Discontinuité transitoire	Discontinuité prolongée ou permanente	Complication médicale ou accidentelle liée à la discontinuité	Décès lié à la discontinuité
Vie privée (RGPD)	Pas d'impact	Quelques désagréments surmontés sans difficulté	Désagréments significatifs surmontés avec quelques difficultés	Conséquences significatives surmontées avec de réelles difficultés	Conséquences significatives voire irrémediables non surmontables
Impact sur l'AP-HP					
Echelle de gravité	1	2	3	4	5
Actifs (informationnels)	Aucune perte d'information	Perte transitoire d'information.	Perte réversible d'information nécessitant d'importants moyens pour leur reconstitution	Perte irréversible d'informations essentielles avec solution de remplacement	Perte irréversible d'informations essentielles sans solution de remplacement
Activité	Aucun impact sur l'activité	Dégradation transitoire de l'activité	Dégradation permanente de l'activité	Arrêt de l'activité, avec solution de remplacement	Arrêt définitif de l'activité
Actifs	Pas de perte financière	Perte ≤ 0,1 %	Perte > 0,1 % et ≤ 1%	Perte > 1 % et ≤ 10 %	Perte > 10 %
Conformité	Observations	Non-conformité mineure	Non-conformité majeure	Interdiction temporaire d'exercer l'activité	Interdiction définitive d'exercer l'activité
Environnement	Aucun impact sur la qualité de l'environnement	Dégradation transitoire de l'environnement local	Dégradation permanente de l'environnement local	Impact à distance transitoire	Impact à distance permanent
Image	Dégrader temporairement l'image de l'AP-HP en interne	Dégrader temporairement l'image de l'AP-HP au niveau régional	Dégrader temporairement la réputation de l'AP-HP au niveau national	Dégrader durablement la réputation de l'AP-HP au niveau national	Dégrader durablement la réputation de l'AP-HP au niveau mondial
Juridique	Absence de réclamation	Réclamation non contentieuse	Risque de réclamation indemnitaire	Réclamation indemnitaire ou risque de réclamation pénale	Réclamation pénale

Modèle de Plan d'Assurance Sécurité (PAS)

- 1 PRESENTATION DU DOCUMENT
 - 1.1 OBJET
 - 1.2 GLOSSAIRE ET DEFINITIONS
 - 1.3 DOCUMENTS DE REFERENCE ET ASSOCIES
- 2 DESCRIPTION DES PRESTATIONS
 - 2.1 OBJECTIFS
 - 2.2 DONNEES TRAITEES
 - 2.2.1 Données
 - 2.2.2 Données personnelles
 - 2.2.3 Données de santé
 - 2.3 SYSTEMES D'INFORMATIONS MIS EN ŒUVRE
 - 2.4 SOUS-TRAITANTS
 - 2.5 EXIGENCES DE SECURITE
- 3 ORGANISATION DE LA SECURITE
 - 3.1 ROLES ET RESPONSABILITES
 - 3.1.1 Responsable sécurité
 - 3.1.2 DPO
 - 3.1.3 Autres responsables
 - 3.1.4 Rôles et fonctions des autres intervenants
 - 3.2 COMITOLOGIE
 - 3.3 PROCEDURES D'EVOLUTION DU PAS
- 4 MESURES DE SECURITE
 - 4.1 SECURITE DES RESSOURCES HUMAINES
 - 4.1.1 Gestion des compétences du projet
 - 4.1.2 Gestion des arrivées départ sur le projet
 - 4.1.3 Sensibilisation et formation à la SSI
 - 4.2 GESTION DES ACTIFS
 - 4.2.1 Cartographie des actifs
 - 4.2.2 Classification des actifs
 - 4.2.3 Protection des informations
 - 4.3 GESTION DES ACCES LOGIQUES
 - 4.3.1 Gestion des rôles
 - 4.3.2 Gestion des habilitations
 - 4.3.3 Attributions des droits d'accès
 - 4.3.4 Contrôle d'accès logique aux SI
 - 4.3.5 Gestion des sessions inactives
 - 4.3.6 Traçabilité des accès
 - 4.4 GESTION DES AUTHENTIFIANTS
 - 4.4.1 Gestion des mots de passe
 - 4.4.2 Gestion des certificats électroniques
 - 4.5 SECURITE PHYSIQUE
 - 4.5.1 Bureaux
 - 4.5.1.1 Zones de sécurité physique
 - 4.5.1.2 Contrôle d'accès physique aux locaux
 - 4.5.1.3 Traçabilité des accès physiques aux locaux
 - 4.5.2 Hébergement informatique
 - 4.5.2.1 Contrôle des accès
 - 4.5.2.2 Surveillance et traçabilité
 - 4.5.2.3 Gestion de l'hébergement (sécurité incendie, électricité, climatisation...)
 - 4.6 SECURITE DE L'EXPLOITATION DES SI
 - 4.6.1 Durcissement des ressources informatiques
 - 4.6.2 Sauvegardes et restauration

- 4.6.3 Documentation des ressources informatiques
- 4.6.4 Gestion des correctifs de sécurité
- 4.6.5 Lutte contre les codes malveillants
- 4.6.6 Administration des SI
- 4.7 SECURITE DES COMMUNICATIONS
 - 4.7.1 Politique de sécurité des communications
 - 4.7.2 Sécurisation des transmissions de données
 - 4.7.3 Accès à distance aux SI
 - 4.7.4 Accès au réseau interne depuis des équipements non maîtrisés
- 4.8 SECURITE DES DEVELOPPEMENTS
 - 4.8.1 Règles de développement et prise en compte de la sécurité
 - 4.8.2 Sécurité du système de développement
 - 4.8.3 Cloisonnement des environnements
 - 4.8.4 Données d'essai
 - 4.8.5 Gestion des évolutions
- 4.9 MAINTENANCE DES SI
 - 4.9.1 Maintien du niveau de sécurité des SI
 - 4.9.2 Sécurité de la maintenance des SI
 - 4.9.3 Mise au rebut
- 4.10 RELATION AVEC LES TIERS
 - 4.10.1 Gestion de la sécurité avec les sous-traitants
- 4.11 GESTION DES INCIDENTS ET DES ALERTES
 - 4.11.1 Veille et gestion des vulnérabilités techniques
 - 4.11.2 Détection et dispositif de gestion des incidents
 - 4.11.3 Journalisation des incidents et des alertes
 - 4.11.4 Gestion de crise
- 4.12 GESTION DE LA CONTINUITE D'ACTIVITE
 - 4.12.1 Définition, mise en œuvre et maintien du plan de continuité d'activité
 - 4.12.2 Protection des données de sauvegarde
- 4.13 MISE A JOUR DES SYSTEMES ET LOGICIELS
 - 4.13.1 Sécurité des postes de travail
 - 4.13.2 Utilisation de terminaux personnels
 - 4.13.3 Privilèges des utilisateurs sur les postes de travail
 - 4.13.4 Stockage des informations
 - 4.13.5 Protection des données critiques
 - 4.13.6 Configuration du navigateur internet
- 4.14 GESTION DE LA DOCUMENTATION
 - 4.14.1 Référentiel documentaire
 - 4.14.2 Gestion de la documentation
- 4.15 CONTROLE ET EVALUATION
 - 4.15.1 Contrôles récurrents de techniques et de conformité
 - 4.15.2 Audits ponctuels de conformité techniques
 - 4.15.3 Reporting SSI
- 5 COUVERTURE DES EXIGENCES DE SECURITE
- 6 DOCUMENTATION DE SUIVI

Modèle de questionnaire de surveillance, révision et gestion des changements des services fournisseurs – Version 3.0

Il convient que l'organisation procède régulièrement à la surveillance, à la révision, à l'évaluation et à la gestion des changements des pratiques de sécurité de l'information du fournisseur et de prestation de services.

Objectif : Maintenir un niveau convenu de sécurité de l'information et de prestation de services, conformément aux accords conclus avec les fournisseurs.

Questions	Réponses
1 Coordonnées	
Section relative à l'identification du fournisseur	
1.1 Pourriez-vous préciser la dénomination ou raison sociale, le n° SIREN et votre adresse postale du siège français ?	
1.2 Pourriez-vous désigner un point de contact (Personne à contacter pour plus d'informations) ? NOM, Prénom, Adresse électronique, Téléphone, Fonction	
2 Politique de sécurité	
Section relative à la politique de conformité au RGPD du sous-traitant.	
2.1 Au cours des 12 derniers mois, avez-vous modifié ou mise à jour vos politiques et procédures de sécurité de l'information ?	<input type="checkbox"/> Oui <input type="checkbox"/> Non
2.2 Pourriez-vous décrire succinctement les modifications ou mises à jour apportées à vos politiques de sécurité ou procédures de sécurité ?	
3 Ressources humaines	
Section relative aux mesures liées aux ressources humaines	
3.1 Au cours des 12 derniers mois, les coordonnées du DPO (Délégué à la Protection des Données), du RSSI (Responsable de la Sécurité du Système d'Information) ou du responsable contractuel ont-elles changées ?	<input type="checkbox"/> DPO <input type="checkbox"/> RSSI <input type="checkbox"/> Responsable contractuel <input type="checkbox"/> Les coordonnées du DPO, du RSSI et du responsable contractuel sont inchangées
3.2 Merci d'indiquer leurs nouvelles coordonnées (Nom, Prénom, téléphone, adresse électronique)	
3.3 Au cours des 12 derniers mois, avez-vous mené des actions de sensibilisation des collaborateurs à la réglementation RGPD et à la sécurité de l'information ?	<input type="checkbox"/> Oui <input type="checkbox"/> Non
3.4 Pourriez-vous décrire succinctement les actions de sensibilisation réalisées ainsi que les catégories et le nombre de collaborateurs en ayant bénéficié ?	
4 Sécurité physique	
Section relative à l'accès aux locaux, aux installations et aux systèmes informatiques du sous-traitant.	
4.1 Au cours des 12 derniers mois, avez-vous effectué des changements d'emplacement physique des installations des services ?	<input type="checkbox"/> Oui <input type="checkbox"/> Non
Indiquer en commentaire le pays ou la zone géographique d'hébergement	
4.2 Au cours des 12 derniers mois, avez-vous effectué des changements en matière de mesures prises pour contrôler l'accès aux locaux ?	<input type="checkbox"/> Oui <input type="checkbox"/> Non
4.3 Pourriez-vous décrire succinctement les changements apportés en matière de mesures prises pour contrôler l'accès aux locaux ?	
5 Services & applications	
5.1 Pourriez-vous communiquer les rapports de service produits au cours de la période écoulée ?	Joindre un document à ce questionnaire
5.2 Au cours des 12 derniers mois, avez-vous apporté des améliorations en matière de sécurité de l'information aux services fournis existants ?	<input type="checkbox"/> Oui <input type="checkbox"/> Non
5.3 Pourriez-vous décrire succinctement les améliorations apportées en matière de sécurité ?	

5.4 Au cours des 12 derniers mois, avez-vous développé de nouvelles applications ou de nouveaux systèmes/services dans le cadre de vos prestations ?	<input type="checkbox"/> Oui <input type="checkbox"/> Non
5.5 Pourriez-vous décrire succinctement ces nouvelles applications et nouveaux systèmes/services ?	
5.6 Au cours des 12 derniers mois, avez-vous utilisé de nouveaux outils et environnements de développement ?	<input type="checkbox"/> Oui <input type="checkbox"/> Non
5.7 Pourriez-vous décrire succinctement les nouveaux outils et environnements de développement ?	
5.8 Au cours des 12 derniers mois, avez-vous mis en œuvre de nouveaux produits ou de versions plus récentes ?	<input type="checkbox"/> Oui <input type="checkbox"/> Non
5.9 Pourriez-vous décrire succinctement les nouveaux produits ou de versions plus récentes des services ?	
5.10 Au cours des 12 derniers mois, avez-vous adopté de nouvelles technologies ?	<input type="checkbox"/> Oui <input type="checkbox"/> Non
5.11 Pourriez-vous décrire succinctement les nouvelles technologies adoptées ?	
5.12 Au cours des 12 derniers mois, avez-vous apporté des changements ou des améliorations de sécurité de l'information aux réseaux ?	<input type="checkbox"/> Oui <input type="checkbox"/> Non
5.13 Pourriez-vous décrire succinctement les changements ou les améliorations de sécurité de l'information aux réseaux ?	
5.14 Pourriez-vous communiquer les rapports d'audit de sécurité de l'information d'auditeurs indépendants, s'ils existent, relatifs aux prestations ?	Joindre un document à ce questionnaire
6 Incidents de sécurité de l'information	
Section relative aux Incidents de sécurité de l'information	
6.1 Au cours des 12 derniers mois, avez-vous subi un ou des incidents de sécurité ayant impacté les prestations délivrées à l'AP-HP ?	<input type="checkbox"/> Oui <input type="checkbox"/> Non
6.2 Pourriez-vous décrire succinctement le ou les incidents de sécurité de l'information ayant impactés les prestations délivrées à l'AP-HP ?	
6.3 Au cours des 12 derniers mois, avez-vous pris des mesures de sécurité nouvelles ou modifiées pour résoudre les incidents de sécurité de l'information et pour améliorer la sécurité de l'information ?	<input type="checkbox"/> Oui <input type="checkbox"/> Non
6.4 Pourriez-vous décrire succinctement les mesures de sécurité nouvelles ou modifiées pour résoudre les incidents de sécurité de l'information et pour améliorer la sécurité de l'information ? ?	
7 Sous-traitance	
Section relative à la conformité de mise en œuvre des activités de traitement du sous-traitant.	
7.1 Au cours des 12 derniers mois, avez-vous sous-traité à d'autres fournisseurs des prestations ?	<input type="checkbox"/> Oui <input type="checkbox"/> Non
7.2 Au cours des 12 derniers mois, avez-vous changé de sous-traitant(s) ?	<input type="checkbox"/> Oui <input type="checkbox"/> Non
7.3 Merci d'indiquer leurs coordonnées (Raison sociale, adresse électronique, adresse postale) et nature des prestations sous-traitées	

Documents de référence

- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) Modifié par le Rectificatif au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) [JOUE L127 2 du 23/05/2018](#)
- Référentiel de certification Hébergeur de données de santé (HDS) - Version : v2.0 - Avril 2024 <https://esante.gouv.fr/services/hebergeurs-de-donnees-de-sante/les-referentiels-de-la-procedure-de-certification>
- Politique générale de la sécurité de l'information de l'AP-HP (PGSI)
- Cadre de cohérence technique du système d'information de l'AP-HP

Directives de sécurité prises en application de la PGSI de l'AP-HP :

- DIRECTIVE – Organisation de la sécurité de l'information
- DIRECTIVE – Sécurité des ressources humaines
- DIRECTIVE – Gestion des actifs
- DIRECTIVE – Sécurité des accès logiques
- DIRECTIVE – Cryptographie
- DIRECTIVE – Sécurité physique et environnementale
- DIRECTIVE – Sécurité liée à l'exploitation
- DIRECTIVE – Sécurité des communications
- DIRECTIVE – Acquisition développement et maintenance des SI
- DIRECTIVE – Sécurité dans les relations avec les Fournisseurs
- DIRECTIVE – Gestion des incidents liés à la sécurité de l'information
- DIRECTIVE – Sécurité de l'information dans la gestion de la continuité
- DIRECTIVE – Conformité des systèmes de traitement de l'information
- DIRECTIVE – Sécurité des services