

PAS : Plan d'assurance sécurité

Sommaire

1	Objet du document	4
2	Documents de référence	4
3	Obligations du prestataire.....	4
4	Localisation des données.....	4
5	Convention de service	4
6	Exigences Générales	5
7	EXIGENCES GENERALES SUR LES LOGICIELS	6
8	IDENTITES	7
9	AUTHENTIFICATION ET SINGLE SIGN ON	7
10	GESTION DES HABILITATIONS.....	8
11	TRACABILITE.....	8
12	PROTECTION DES SYSTEMES	10
13	CRYPTOGRAPHIE.....	11
14	MAINTENANCE ET TELEMANTENANCE	11
15	PROTECTION DES DONNEES MEDICALES	14
16	CAS PARTICULIER SELON LE PERIMETRE	14
16.1	Cas de moyens mobiles :	14
16.2	Cas de services Hébergés.....	15
16.2.1	Concernant l'accès au service hébergé par des utilisateurs du CHU de Nice :	16
16.2.2	Concernant la continuité du service hébergé :	16
16.2.3	Concernant la réversibilité du service hébergé :	17
16.2.4	Concernant la garantie de Confidentialité des données hébergées :	17
16.2.5	Règles supplémentaires en cas d'installation dans l'infrastructure du CHUN	18
17	GLOSSAIRE.....	19
18	ENGAGEMENT DE L'ORGANISME	20

INTRODUCTION

Le Plan d'Assurance Sécurité (PAS), annexé aux Cahiers des Clauses Techniques Particulières (CCTP) des marchés du CHU de NICE/du GHT06, a pour objectif d'évaluer le niveau de sécurité et la conformité des solutions proposées, par rapport aux exigences réglementaires issues de l'Arrêté du 18 Septembre 2018 publié au JORF n°2023 du 27 Septembre 2018, ainsi qu'à la Politique de Sécurité des Systèmes d'Information propres au CHU de NICE/ au GHT06 .

Document contractuel, il décrit l'ensemble des dispositions spécifiques que les candidats s'engagent à mettre en œuvre pour garantir le respect des exigences de sécurité du pouvoir adjudicateur .

C'est aussi un cadre de réponse : il offre une structure pour la réponse des candidats aux exigences de sécurité, ce qui permet de mieux évaluer la pertinence de la couverture des exigences.

Dans les marchés spécifiquement visés, le PAS pourra constituer un critère de jugement des offres soumis à notation. Il facilite ainsi la comparaison entre les différentes offres. Une fois le prestataire retenu, le PAS est annexé au contrat et devient une pièce de marché. Il se substitue aux éventuelles clauses génériques de sécurité du prestataire. Le plan-type proposé ci-après doit être joint au DCE comme base de rédaction du Plan d'Assurance Sécurité qui sera complété et remis par les candidats lors de la soumission à la consultation.

Les solutions informatiques déployées au sein du Système d'Information du /GHT06 ?doivent :

- Satisfaire les exigences de sécurité informatique définies dans la Politique de Sécurité des Systèmes d'Information du CHU de Nice / GHT06 ?.
- Respecter les préconisations en matière de sécurité de l'ASIP Santé, l'ANSSI et du Ministère de la santé (PSSI –MCAS qui pourra être fournie sur demande).
- Respecter les exigences complémentaires propres à des systèmes critiques spécifiques

Les **exigences de sécurité sont obligatoires** leur non-respect est éliminatoire et elles sont notées **O comme Obligatoire (en début d'exigence) dans ce document.**

- Toutes les cases « description de la prise en charge » doivent être renseignées. Si une règle n'est pas applicable la mention N/A est inscrite et doit être justifiée.
- Elles seront prises en compte dans l'évaluation technique de l'offre pour les consultations où le PAS est un critère de jugement des offres.

Les présentes exigences de sécurité seront intégrées dans la convention/le marché/le contrat conclu avec le CHU de Nice le cas échéant et s'imposeront dans le cadre de son exécution.

Le titulaire doit respecter les précautions mentionnées dans le guide de sécurité des données personnelles de la CNIL Edition 2018 et les exigences issues du Règlement Général pour la Protection des Données (RGPD).

- Si vous n'êtes pas concerné, merci de remplir l'encart ci-dessous :

☐ J'atteste ne pas être concerné par l'annexe PAS

Fait à

Le

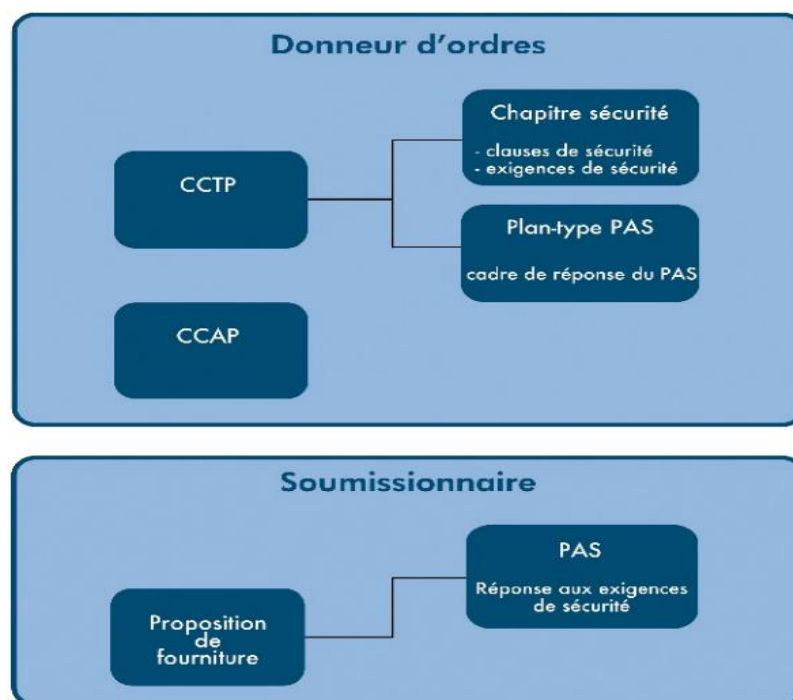
Pour l'établissement.....

En qualité de

Nom, prénom.....

Signature,

Pour tout complément d'information sur ce document, vous pouvez contacter le Responsable Sécurité du Système d'Information du CHU Nice à l'adresse mail suivante : RSSI@chu-nice.fr



1 Objet du document

Le présent document décrit les dispositions que les candidats s'engagent à mettre en œuvre pour répondre aux exigences de sécurité du CHU de Nice/ GHT06. Il définit en particulier l'organisation qui sera mise en place, la méthodologie à suivre pour gérer la sécurité du projet d'externalisation et les mesures techniques, organisationnelles et procédurales qui seront mises en œuvre.

2 Documents de référence

Ce paragraphe liste les documents de référence pour le Plan d'Assurance Sécurité.

Les documents applicables seront les suivants :

- Le contrat (CCTP, CCAP) ;
- Le cahier des charges, incluant les exigences de sécurité du CHU de Nice/ GHT06 ;

3 Obligations du candidat

Le candidat reconnaît être tenu à une obligation de conseil, de mise en garde et de recommandations en termes de sécurité et de mise à l'état de l'art. En particulier il s'engage à informer le pouvoir adjudicateur des risques d'une opération envisagée, des incidents éventuels ou potentiels, et de la mise en œuvre éventuelle d'actions correctives ou de prévention. Outre le respect de ses obligations au titre de la convention de service, le prestataire/candidat informera préalablement le client/le pouvoir adjudicateur de toute opération susceptible de provoquer l'indisponibilité (ou une dégradation des performances) du système. Le prestataire/candidat est responsable du maintien en condition de sécurité du système pendant toute la durée des prestations. Les mécanismes de sécurité mis en œuvre doivent évoluer conformément à l'état de l'art : la découverte de failles dans un algorithme, un protocole, une implémentation logicielle ou matérielle, ou encore l'évolution des techniques de cryptanalyse et des capacités d'attaque par force brute doivent être pris en compte.

4 Localisation des données

Les lieux d'hébergement des données doivent satisfaire aux exigences de sécurité du donneur d'ordres et aux dispositions de la loi du 6 janvier 1978 modifiée, relative à la protection des données personnelles. Le prestataire/candidat doit communiquer la liste de tous les lieux de stockage de données (site d'hébergement principal, site(s) de secours, etc.). Si la faisabilité technique de cette exigence peut s'avérer délicate dans le cadre d'architectures distribuées, il peut être demandé au prestataire/candidat/attributaire d'être en mesure de localiser, a posteriori, et non en permanence, le lieu de stockage des données, en particulier suite à un incident. Cette clause pourra être complétée par un certain nombre d'exigences, permettant notamment de garantir une bonne accessibilité des sites d'hébergement.

5 Convention de service

Cette clause est la formalisation d'un accord entre le prestataire titulaire et le client/pouvoir adjudicateur relatif au niveau de service attendu (Service Level Agreement). Ainsi, il pourra être demandé au prestataire candidat/ titulaire des engagements concernant :

- Le taux de disponibilité du système (en heures ouvrées / non ouvrées) ;

- La durée et l'occurrence maximale d'indisponibilité mensuelle, trimestrielle ou annuelle d'un composant ou du système ;
- Le temps de réponse d'une application ou de certaines requêtes, la durée maximale de certains traitements ;
- Le temps garanti d'intervention sur site (GTI) ;
- Le temps garanti de remise en état d'un composant matériel ou logiciel défectueux (GTR), ou d'une chaîne de liaison ;
- Le temps moyen entre deux pannes (MTBF) ;
- Le taux de panne mensuel, trimestriel ou annuel d'un composant ou du système (taux de fiabilité).

Ces engagements pourront être définis pendant une phase probatoire, et réajustés à l'issue de celle-ci. Ils pourront également être redéfinis en cas de modification du périmètre de l'opération. Les niveaux d'engagement, de même que les pénalités en cas de non-respect de ces derniers, seront négociés selon les spécificités de chaque projet.

Les solutions informatiques déployées au sein du Système d'Information du CHU de Nice GHT06 ? doivent :

- Satisfaire les exigences de sécurité informatique définies dans la Politique de Sécurité des Systèmes d'Information du CHU de Nice GHT06 ?.
- Respecter les préconisations en matière de sécurité de l'ANS, l'ANSSI et du Ministère de la santé (PSSI –MCAS qui pourra être fournie sur demande).
- Respecter les exigences complémentaires propres à des systèmes critiques spécifiques

6 Exigences Générales

Les **exigences de sécurité sont obligatoires (O)** leur non-respect est éliminatoire

- Toutes les cases « description de la prise en charge » doivent être renseignées. Si une règle n'est pas applicable, la mention N/A est inscrite et doit être justifiée.

Les présentes exigences de sécurité seront intégrées dans le marché conclu avec le CHU de Nice GHT06 ? le cas échéant et s'imposeront dans le cadre de son exécution.

Le titulaire doit respecter les précautions mentionnées dans le guide de sécurité des données personnelles de la CNIL Edition 2018 et les exigences issues du Règlement Général pour la Protection des Données (RGPD).

Le titulaire doit respecter l'Arrêté du 18 septembre 2018 portant approbation du cahier des clauses simplifiées de Cybersecurity

EXIGENCES GENERALES SUR LES LOGICIELS

	Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
O	2.0	Le titulaire s'engage à acquérir et à concéder à l'ÉTABLISSEMENT l'ensemble des licences d'utilisation nécessaires au bon fonctionnement du dispositif connecté, sauf conditions spécifiques. Ceci concerne l'ensemble des logiciels et couches logiques utilisées (OS, progiciels, BDD, télémaintenance...).		
O	2.1	Le titulaire s'engage à fournir la liste exhaustive des logiciels installés, documentée (niveau de version, prérequis, ...) et contenant les informations détaillant chaque logiciel ainsi que les interactions entre eux.		
O	2.2	Pour tout ce qui est fourni au titre de l'offre, le titulaire s'engage à acquérir et à concéder au CHU de Nice l'ensemble des licences d'utilisation nécessaires à son bon fonctionnement. Si nécessaire, il détaillera les conditions spécifiques ou exclusions. Ceci concerne l'ensemble des logiciels et couches logiques utilisées (OS, progiciels, BDD, télémaintenance...).		
O	2.3	Le titulaire s'engage à n'installer et n'activer que les seuls logiciels nécessaires au bon fonctionnement du dispositif objet du marché.		
O	2.4	Pour les logiciels libres, la conformité du logiciel est de la responsabilité du titulaire seul. Ils devront aussi respecter les exigences de sécurité.		
O	2.5	Pour les logiciels gratuits, la conformité du logiciel est de la responsabilité du titulaire seul : ils devront aussi respecter les exigences de sécurité.		

	Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
O	2.6	Pour les logiciels de type SaaS (Software as a Service : logiciel hébergé), la conformité du logiciel est de la responsabilité du titulaire seul : ils devront aussi respecter les exigences de sécurité.		
O	2.7	Les personnels du titulaire devront signer et respecter la CHARTRE DE CONFIDENTIALITÉ ET DE SÉCURITÉ POUR LES INTERVENANTS EXTERNES lors de toute intervention à l'installation ou en maintenance. Le titulaire s'engage à en informer ses personnels.		
O	2.8	Toute opération réalisée par le titulaire et ses personnels lors de l'installation devra respecter les mêmes règles que celles décrites dans le chapitre Maintenance et Télémaintenance durant son exécution.		
O	2.15	Si la solution proposée entre dans le périmètre de sous-traitant du Règlement Général européen sur la Protection des Données (RGPD), le titulaire devra respecter ce règlement à date d'application et accepter des audits de vérification de conformité. Les clauses spécifiques au RGPD fournies en annexe dédiée doivent être signées par le représentant légal du sous-traitant.		
O	2.16	Aucune version de système d'exploitation non maintenue par l'éditeur en termes de mise à jour de sécurité ne devrait être installée sauf cas particulier nécessitant une protection supplémentaire à décrire.		

7 IDENTITES

Le CHU de Nice a pris le parti d'établir le service d'annuaire de la société Microsoft (AD : Active Directory) en référentiel garant de l'unicité des comptes utilisateurs

8 AUTHENTIFICATION ET SINGLE SIGN ON

Le CHU de Nice n'envisage l'authentification unique (Single Sign On) qu'au travers de l'identité de domaine portée par les protocoles communément utilisés en environnement Windows.

	Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
O	4.1	Les mots de passe des comptes nécessaires à l'administration de la solution doivent pouvoir être modifiés par le CHU de Nice.		
O	4.5	Pour les applications web exposées sur internet et qui intégreraient une authentification et/ou une gestion des comptes : Les pages réservées à l'authentification et à la création de comptes devront intégrer un dispositif de prémunition contre l'usage de robots.		
O	4.6	Pour les applications web exposées sur internet et qui intégreraient une authentification et/ou une gestion des comptes, les mécanismes d'authentification doivent être adaptés à la criticité des données. Une authentification forte est exigée pour l'accès à des données de santé par carte CPS ou équivalent (sauf disposition contraire du CCTP qui conduirait le CHU de Nice à prendre en charge une authentification forte en préalable à l'accès à l'application objet du marché : cas d'un portail d'authentification en amont de l'application).		

9 GESTION DES HABILITATIONS

10 TRACABILITE

Les exigences fonctionnelles de traçabilité du CCTP peuvent être supérieures à celle citées ici d'une manière générale pour la sécurité.

- Le CHU de Nice GHT06 ? souhaite mettre en œuvre la centralisation de ses traces applicatives et systèmes au sein d'un dispositif unique afin d'en garantir l'intégrité, la conservation et la bonne exploitation et protection

Contenu de la Trace

	Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
O	5.2	La capacité (ou non) à tracer toutes les actions (y compris la consultation de données) doit être décrite.		
O	5.3	Les accès utilisateurs (et administrateurs) seront tracés en réussite et en échec.		
O	5.4	Dans le cadre de systèmes gérant des données personnelles les traces de consultation et de modification sont obligatoires.		
O	5.5	Les traces produites devront être accessibles par l'outil de centralisation des traces du CHU de Nice dans un format et un mode d'accès rendus possibles et décrits par le titulaire (ATNA : format IHE, syslog, requête dans une base de données à fournir, fichier à décrire).		

11 PROTECTION DES SYSTEMES

	Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
O	6.1	<p>Le titulaire s'engage à mettre en œuvre les dispositifs et paramétrages nécessaires pour prémunir ses systèmes contre les attaques virales et intrusives selon l'une des formes suivantes :</p> <ul style="list-style-type: none"> • Déploiement de ses propres utilitaires et politiques de mise à jour. • Intégration de ses dispositifs dans la démarche sécurité du CHU de Nice en installant l'antivirus du CHUN et en inscrivant ses systèmes dans les règles de gestion des correctifs de sécurité en vigueur pour le reste du SI. • Les types de fichiers nécessitant une exclusion d'analyse par l'antivirus conditionnant le bon fonctionnement doivent être communiqués pour décider d'un éventuel complément de sécurité • A défaut, ou en cas d'une insuffisance de l'analyse antivirale, une solution de sécurité externe en interface avec le dispositif objet du marché sera installée (équipement de type pare-feu avec antivirus). <p>De fait, en cas d'intrusion ou de contamination, le titulaire est responsable de la vulnérabilité de ses systèmes vis à vis des définitions virales et correctifs publics.</p>		

12 CRYPTOGRAPHIE

Lorsqu'une télémaintenance est prévue par le titulaire, des règles strictes doivent être prises en compte :

	Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
O	7.1	Dans le cas d'applications web publiées sur internet comme sur l'intranet, l'usage de SSL est impératif. Le titulaire pourra recourir à des certificats fournis par le CHU de Nice		
O	7.2	Les données utiles à l'authentification doivent être chiffrées lors de leur communication et de leur stockage.		
O	7.3	De manière générale, si des techniques cryptographiques sont utilisées, elles doivent être conformes aux standards du marché, et au Référentiel Général de Sécurité (RGS).		

13 MAINTENANCE ET TELEMaintenance

Lorsqu'une télémaintenance est prévue par le titulaire, des règles strictes doivent être prises en compte :

	Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
O	8.1	Pour ce qui concerne la remontée d'informations issues des dispositifs maintenus vers votre site de diagnostic, cet envoi doit être décrit précisément en indiquant toutes les données transférées. Cet usage exclusif à des fins de surveillance du maintien en condition opérationnelle et l'absence de données personnelles directement ou indirectement liées à nos patients doivent être garantis. Cette remontée d'information devra utiliser des protocoles sécurisés, être tracée et passer par nos passerelles de contrôle d'accès à internet ou par un VPN IPSEC site à site avec votre site de télédiagnostic (recommandé).		
O	8.2	La connexion de télémaintenance doit se faire via la passerelle Internet sécurisée mise à disposition par le CHU de Nice (Solution IpDiva de Systancia). La demande d'accès devra suivre la procédure du CHU de Nice.		

	Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
O	8.3	Au niveau des postes de travail standard du CHU de Nice, aucun outil de prise de contrôle à distance ne peut être installé dans le cadre d'une application. Le seul outil de prise à contrôle à distance autorisé est celui servant à l'administration système gérée par la DINSI du CHU de Nice.		
O	8.4	Il est de la responsabilité du titulaire d'assurer la sécurité de sa plateforme d'intervention à distance (données et logiciels)		
O	8.5	Le CHU de Nice se réserve le droit de faire (ou de faire faire) des contrôles de sécurité de façon périodique ou ponctuelle chez le titulaire afin de s'assurer que le niveau de sécurité requis est conforme aux exigences de sécurité en vigueur.		
O	8.6	le titulaire doit avoir une politique anti-virus et de mise à jour des correctifs de sécurité appliquée sur les postes de télémaintenance.		
O	8.8	les données à caractère personnel ou technique du CHU de Nice (configuration des équipements) exploitées par les équipes de support chez le titulaire ne doivent pas être divulguées (une protection adaptée doit être réalisée).		
O	8.9	L'intervention de maintenance est encadrée par un règlement, une charte, un contrat ou une convention entre le CHU de Nice et le titulaire, définissant les engagements de chacun, les modalités pratiques, ...		
O	8.10	Le titulaire s'engage sur la sécurité de la prestation, son représentant légal devra signer l'engagement titulaire de maintenance fourni par la DINSI rappelant la confidentialité des données et l'engageant à informer ses personnels que tous les accès et actions seront tracés.		
O	8.11	Il est de la responsabilité du titulaire de restreindre les accès physiques et logiques de ses postes aux seules personnes autorisées (par sensibilisation et mise à disposition de moyens de sécurité adéquats).		
O	8.12	Il est de la responsabilité du titulaire de connaître en toutes circonstances l'identité de toute personne qui se connecte ou s'est connectée sur la plateforme de télémaintenance et d'en assurer la traçabilité (cette traçabilité pourra être communiquée sur demande du CHU de Nice).		

	Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
O	8.13	Il est de la responsabilité du titulaire de veiller à ce que toutes les informations résiduelles inutiles à l'issue d'une intervention soient supprimées.		
O	8.14	Le titulaire réalise un suivi permanent des incidents et vulnérabilités liés aux dispositifs connectés et met à disposition les correctifs et préventifs nécessaires dans les délais appropriés.		
O	8.15	Le titulaire s'engage à effectuer des tests de robustesse et de non-régression à chaque évolution du matériel ou du logiciel. Les impacts d'une défaillance qui serait néanmoins constatée seraient de la responsabilité du titulaire, la correction et la prise en charge des impacts à sa charge.		
O	8.17	Le titulaire doit fournir un rapport détaillé de l'intervention effectuée.		
O	8.18	Si le CHU de Nice dispose d'une solution de type « bastion d'administration », ou le met en place ultérieurement, le titulaire s'engage à l'utiliser pour accéder aux systèmes qu'il devra maintenir ou exploiter (de fait l'accès direct aux serveurs et applications est interdit). Selon les besoins d'intervention, l'accès aux systèmes à maintenir ou exploiter sera ouvert et fermé par la DINSI à la demande (du mainteneur ou de la personne habilitée, selon le protocole défini dans les conditions de la maintenance). Si l'établissement ne dispose pas d'un bastion d'administration, le cas d'utilisation d'un bastion équivalent du titulaire pourra être étudié s'il apporte les mêmes garanties de protection, de traçabilité, de preuve opposable et d'accès avec la possibilité d'audit (une description précise devra être fournie).		
O	8.20	l'authentification forte de la CNIL : complexité du mot de passe, changement à la 1ère connexion, renouvellement automatique, verrouillage ou déconnexion au bout d'un délai, blocage du compte au bout de X accès infructueux,		
O	8.21	Le titulaire établira les procédures d'archivage, épuration des données pour respecter les délais de conservation des données		

14 PROTECTION DES DONNEES MEDICALES

	Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
0	10.1	Le titulaire et son personnel, le personnel du CHU de Nice sont soumis à un engagement de confidentialité conformément aux préconisations de la CNIL et au Code de la Santé Publique. Ces articles s'adressent notamment aux titulaires extérieurs. Qui s'engagent à signer et respecter la charte d'accès et d'usage au SI des intervenants extérieurs.		

Article L1110-4 du Code de la Santé Publique

....Excepté dans les cas de dérogation expressément prévus par la loi, ce secret (secret médical) couvre l'ensemble des informations concernant la personne venues à la connaissance du professionnel de santé, de tout membre du personnel de ces établissements, services ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes. Il s'impose à tout professionnel de santé ainsi qu'à tous les professionnels intervenant dans le système de santé.

	Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
0	10.2	En conséquence, notamment, les jeux de données éventuellement fournies par le CHU de Nice sont strictement confidentiels et sont liés au secret professionnel.		

15 CAS PARTICULIER SELON LE PERIMETRE

15.1 Cas de moyens mobiles :

	Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
0	11.1	Tout dispositif mobile doit être chiffré (en conformité avec le Référentiel Général de Sécurité : RGS) et les clefs de chiffrement doivent être remises au CHU de Nice.		

15.2 Cas de services Hébergés

Service hébergé en dehors du Système d'information de la DINSI (pour tout ou partie de l'objet du marché) et cas de services installés dans le SI du CHU de Nice mais administrés en autonomie par le titulaire (cas SaaS)

	Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
O	11.2	Si le centre de maintenance ou d'hébergement est en dehors du territoire national cela devra être précisé pour analyser les contraintes réglementaires associées au type de système à protéger selon la politique de sécurité de l'état et du ministère de rattachement. Le candidat doit préciser les pays où sont réalisés les hébergements. Dans le cas d'hébergement hors communauté européenne les dispositions adaptées doivent être préalablement réalisées et validées par les autorités compétentes.		
O	11.3	Si des données de santé sont hébergées chez le titulaire ou un de ses sous-traitants celui-ci doit être agréé hébergeur de données de santé par l'ANS (ou toute commission compétente désignée par la réglementation).		
O	11.4	Si la solution proposée entre dans le périmètre de sous-traitant du Règlement Général européen sur la Protection des Données (RGPD), le titulaire devra respecter ce règlement à date d'application et accepter des audits de vérification de conformité. A cette fin sont annexées au contrat <i>les clauses de conformité au RGPD</i> .		
O	11.5	Si des données nominatives à caractère personnel font l'objet de traitement par le système, le traitement sera conforme à la loi CNIL et au RGPD et le titulaire devra démontrer le niveau de protection adapté à la criticité de ces données ? Cette démonstration fera l'objet d'un livrable de son offre.		

15.2.1 Concernant l'accès au service hébergé par des utilisateurs du CHU de Nice GHT06 :

	Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
O	11.7	Une authentification d'accès doit permettre aux utilisateurs d'accéder aux services avec un niveau de sécurité adapté aux données à protéger. Les utilisateurs pourront changer leur authentifiant (mot de passe ou moyen d'authentification). La confidentialité des mots de passe doit être garantie par l'hébergeur lors de son stockage (chiffré) et de sa saisie. Pour l'accès aux données de santé l'authentification devra être conforme aux exigences d'authentification forte de la CNIL et de l'ASIP (carte CPS ou équivalent).		
O	11.8	Les mots de passe ne doivent pas être stockés en clair dans le logiciel ou la base de données.		
O	11.9	Le titulaire doit remettre un compte et authentifiant pour audit au RSSI du CHU de Nice et accepte que le CHUN réalise ou commande des audits externes pour vérifier la conformité aux exigences de sécurité.		

15.2.2 Concernant la continuité du service hébergé :

	Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
O	11.10	Le service ne doit pas être indisponible plus que la durée décrite dans le CCTP en nombre d'heures. A défaut le fournisseur titulaire précisera les durées sur lesquelles il s'engage.		

15.2.3 Concernant la réversibilité du service hébergé :

	Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
O	11.12	Une copie exploitable des données (base de données ou fichier informatique avec champs délimités et décrits) est transmise au CHU de Nice 3 mois avant la fin de ce contrat pour permettre la réalisation de tests de migration (mode de mise à disposition à décrire par le fournisseur ou imposé dans le CCTP)		
O	11.13	Une copie exploitable des données (base de données ou fichier informatique avec champs délimités et décrits) est transmise au CHU de Nice en fin de contrat (mode de mise à disposition à décrire par le fournisseur ou imposé dans le CCTP)		

15.2.4 Concernant la garantie de Confidentialité des données hébergées :

	Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
O	11.14	Le titulaire s'engage à garantir un accès aux données aux seules personnes habilitées selon les besoins du CHU de Nice		
O	11.15	Les intervenants sont identifiés et doivent signer la Charte des intervenants Externes. Les accès et actions réalisées pourront être tracés.		
O	11.16	Le titulaire s'engage à détruire les données en fin de contrat après les avoir restituées au CHU de Nice sous une forme exploitable.		

15.2.5 Règles supplémentaires en cas d'installation dans l'infrastructure du CHUN

	Ref.	Règle de sécurité	Description de la prise en charge	Evaluation
O	11.17	Le titulaire doit s'engager à maintenir les composants à niveau en termes de sécurité et garantir une administration sécurisée intégrant au moins un antivirus mis à jour et un système d'exploitation ainsi que tous les composants mis à jour des correctifs de sécurité publiés par les éditeurs selon des modalités de qualification à décrire.		
O	11.18	L'accès depuis l'extérieur du CHU de Nice pour l'exploitation et la maintenance doivent respecter les conditions décrites au paragraphe Maintenance et Télémaintenance.		
O	11.19	Pour tout type de traitement le titulaire doit remettre un compte et authentifiant pour audit au RSSI du CHU de Nice et accepte que le CHUN réalise ou commande des audits externes pour vérifier la conformité aux exigences de sécurité.		
O	11.20	Les échanges avec l'extérieur du CHU de Nice doivent être sécurisés : utilisation de protocoles sécurisés et filtrage et contrôle par les équipements de sécurité du CHU de Nice (le CHUN se réserve le droit de tracer tout accès et action sur les systèmes installés dans son infrastructure.)		

16 GLOSSAIRE

- AD (Active Directory) : Service d'annuaire de la société Microsoft
- Application Web : Architecture applicative reposant sur la mise à disposition par HTTP de contenus HTML dynamiques
- HTTP (Hypertext Transfer Protocol) : protocole de communication client/serveur reposant sur le principe de requête/réponse vis-à-vis de ressources identifiées par une adresse réticulaire
- IAM (Identity and Authorization Manager) : Service de gestion et de synchronisation des identités et autorisations entre les différents composants du système d'information
- Kerberos : Protocole d'authentification reposant sur un chiffrement symétrique
- LDAP (Lightweight Directory Access Protocol) : protocole standard de communication avec un service d'annuaire
- NTLM : Protocole d'authentification reposant sur un mécanisme de challenge
- OWASP : Open Web Application Security Project
- PKI (Public Key Infrastructure): Dispositif de gestion des clefs publiques. Permet l'édition des bi-clefs nécessaires au cryptage asymétrique.
- RGPD : Règlement Général sur la Protection des Données.
- SGBD : Dispositif de dépôt et d'indexation de données permettant l'adressage de grands volumes
- SOAP : Protocole applicatif mis en œuvre dans le cadre de web services reposant sur l'échange de flux XML par le biais d'un serveur HTTP.
- Web Service : Service applicatif exposé sous forme d'API selon le protocole SOAP.
- XML (Extended Markup Language) : « langage de balisage extensible¹ » en français) est un métalangage informatique de balisage générique.

17 ENGAGEMENT DE du candidat/de l'opérateur économique

L' le candidat/ l'opérateur économique paraphe toutes les pages et signe ce document

Fait à , le.../.../...

Pour le candidat/l'opérateur économique
(nom et qualité du signataire et cachet de la société)