

|  |
| --- |
| Politique de Sécurité du Système d’Information |
| Clauses de Sécurité, de Protection des données personnelles et de Confidentialité |
| **Direction du Système d’Information**  Sécurité du Système d’Information |
| Version document : 10/12/2021 |

**Politique de Sécurité du Système d’Information**

Clauses de Sécurité, de Protection des données personnelles et de Confidentialité

**SOMMAIRE**

[A. Objet 3](#_Toc90044855)

[B. Définitions 4](#_Toc90044856)

[I. Abréviation 4](#_Toc90044857)

[II. Définitions contextuelles 5](#_Toc90044858)

[C. Confidentialité 6](#_Toc90044859)

[D. Sécurité 7](#_Toc90044860)

[I. Directive NIS 7](#_Toc90044861)

[II. Certification hébergeur de données de santé du CHU de Rouen 7](#_Toc90044862)

[III. Accès physiques aux locaux 7](#_Toc90044863)

[IV. Vidéoprotection 8](#_Toc90044864)

[V. Mesures liées aux réseaux 8](#_Toc90044865)

[VI. Connexion du matériel du Titulaire sur les réseaux du CHU de Rouen 9](#_Toc90044866)

[VII. Connexion au système d’information du CHU de Rouen par le Titulaire 10](#_Toc90044867)

[VIII. Cartographie des systèmes d’information 10](#_Toc90044868)

[IX. Echanges et communications d’informations 10](#_Toc90044869)

[X. Protection contre les logiciels malveillants 11](#_Toc90044870)

[XI. Gestion des vulnérabilités 11](#_Toc90044871)

[XII. Signalements de sécurité 12](#_Toc90044872)

[XIII. Télémaintenance 12](#_Toc90044873)

[XIV. Téléservices de l’administration électronique 13](#_Toc90044874)

[XV. Homologation de sécurité 13](#_Toc90044875)

[XVI. Personnel du Titulaire 13](#_Toc90044876)

[XVII. Les exigences fonctionnelles de sécurité pour un progiciel 14](#_Toc90044877)

[1. Identification/Authentification 14](#_Toc90044878)

[2. Contrôle d’accès 14](#_Toc90044879)

[3. Journalisation / imputabilité 15](#_Toc90044880)

[4. Protection de l’intégrité du Progiciel 15](#_Toc90044881)

[XVIII. Prestations d’achat de matériels/logiciels 15](#_Toc90044882)

[XIX. Hébergement des données et des services 16](#_Toc90044883)

[XX. Réversibilité, Transférabilité et Destruction des Données 16](#_Toc90044884)

[E. Méthodologie sécurisée d’ingénierie et de développement 17](#_Toc90044885)

[1. Obligations spécifiques liées aux prestations d’étude 17](#_Toc90044886)

[2. Obligations spécifiques liées aux prestations de développement 17](#_Toc90044887)

[F. Etats de l'art 19](#_Toc90044888)

[I. Interfaces web 19](#_Toc90044889)

[II. Services de courriels 19](#_Toc90044890)

[III. Composants techniques 19](#_Toc90044891)

[IV. Appareils connectés 20](#_Toc90044892)

[V. Sauvegardes des données stockées 20](#_Toc90044893)

[VI. Administration des systèmes d'information 20](#_Toc90044894)

[VII. Audit 21](#_Toc90044895)

[G. Annexes 22](#_Toc90044896)

[I. Matrice Impact-Gravité 22](#_Toc90044897)

[II. Documents de référence 23](#_Toc90044898)

1. Objet

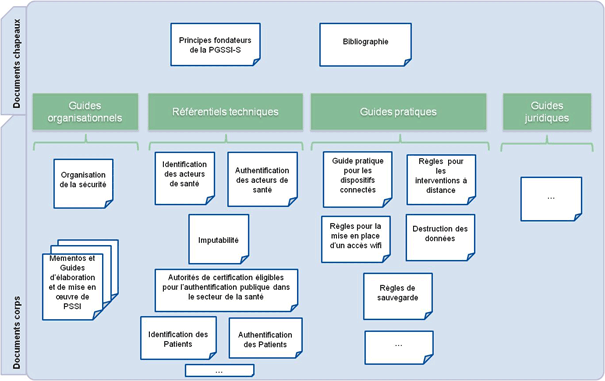
Les solutions et matériels déployés au sein du Système d’Information du Centre Hospitalo-Universitaire de Rouen doivent satisfaire les exigences de sécurité numériques définies dans la politique cadre de sécurité de l’établissement.

Ils doivent, d’autre part, respecter au plus près les préconisations en matière de sécurité de l’ANS, l’ANSSI et du Ministère chargé des Affaires Sociales et de la Santé (PMSSI qui pourra être fournie sur demande).

De même, l’établissement est règlementairement soumis à des opérations d’audits et de certifications (Certification des Comptes, Certification Hôpital Numérique, Certification Haute Autorité de Santé, COFRAC, etc.). Ces obligations sont porteuses de nombreuses exigences, en termes de définition de processus, de respect de procédures et de capacité de traçabilité. La mise en œuvre de ces dispositifs doit permettre d’apporter une réponse appropriée à ces nouvelles exigences, ainsi qu’une amélioration mécanique de la qualité et de la solidité de notre SIH.

Ce document vise à présenter les clauses contractuelles particulières sur la Sécurité du Système d’Information à mettre en œuvre par les prestataires, les fournisseurs et les éditeurs au sein du Centre Hospitalier Universitaire (CHU) de Rouen.

Ce document est un élément complémentaire de la **Politique de Sécurité des Systèmes d’Information**, document fondateur de la démarche de sécurisation des systèmes d’information CHU de Rouen. Il s’inscrit dans le cadre des référentiels spécifiques définis dans la Politique Générale de Sécurité des Systèmes d’Information de Santé (PGSSI-S).



1. Définitions
2. Abréviation

**Active Directory (AD)**

Service d’annuaire de la société Microsoft.

**Agence Nationale de Santé (ANS)**

Groupement d’intérêt public. Ces missions consistent au renforcement de la maîtrise d’ouvrage publique des systèmes d’information et l’accompagnement de l’émergence de technologies numériques dans le secteur de la santé afin d’améliorer l’accès aux soins et veiller au respect des droits des patients.

**Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)**

Autorité nationale en matière de sécurité et de défense des systèmes d'information.

**Application Web**

Logiciel applicatif hébergé sur un serveur et accessible via un navigateur web.

**Carte Professionnelle de Santé (CPS)**

Carte d’identité professionnelle électronique dédiée aux secteurs de la santé et du médico-social.

**Centre Hospitalier et Universitaire (CHU)**

Etablissement hospitalier dans lequel sont prodigués des soins par des professionnels de santé confirmés et des étudiants.

**Commission Nationale de L'Informatique et des Libertés (CNIL)**

Autorité administrative en charge de veiller à ce que l’informatique soit au service du citoyen et qu’elle ne porte atteinte ni à l’identité humaine, ni aux droits de l’homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

**Délégué à la Protection des Données (DPD)**

Référent interne, au regard du règlement européen à la protection des données (RGPD) entré en vigueur le 25 mai dernier, dont le rôle est de veiller au respect du cadre légal concernant la protection des données au sein d'une organisation.

**Direction des Systèmes d’Information (DSI)**

Elle est responsable de l'ensemble des composants matériels (postes de travail, serveurs, équipements de réseau, systèmes de stockage, de sauvegarde et d'impression, etc.) et logiciels du système d'information.

**Endpoint detection and response (EDR)**

Un logiciel de type EDR désigne une technologie de détection des menaces sur les EndPoints (ordinateurs, serveurs).

**Logiciel**

Ensemble des programmes et des procédures nécessaires au fonctionnement d'un système informatique.

**Next-Gen Antivirus (NGAV)**

Logiciel de protection contre les malwares de nouvelle génération.

**Règlement Général sur la Protection des Données (RGPD)**

Règlement de l'Union européenne entré en vigueur à compter du 25 mai 2018. Texte de référence en matière de protection des données à caractère personnel.

**Responsable Sécurité du Système d’Information (RSSI)**

Personne nommée par la Direction Générale dont le rôle est de définir et de veiller à la mise en œuvre de la politique de sécurité au sein de l’établissement.

Au sein de la DSI, le département Méthode, Qualité, Sécurité et Contrôle Interne a été mis en place avec notamment un volet sur la sécurité du SI. Pour tout contact, une liste de distribution est définie : [DSI.RSSI@chu-rouen.fr](mailto:DSI.RSSI@chu-rouen.fr)

**Software as a Service (SaaS)**

Logiciel hébergé.

**Système d’information Hospitalier (SIH) ou Système d’information (SI)**

Ensemble des éléments et règles participant à la gestion, au stockage, au traitement, au transport et à la diffusion de l’information au sein de l’Établissement et vers ses partenaires externes.

**Système de Gestion de Base de Données (SGBD)**

Dispositif de dépôt et d’indexation de données permettant l’adressage de grands volumes

**Web Service**

Service applicatif exposé sous forme d’API selon le protocole SOAP.

1. Définitions contextuelles

Aux fins d’exécution du présent marché, 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 au 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 toutes les pièces ce rapportant au présent marché et à son exécution.

Aux fins d’exécution du présent marché, les définitions de la norme NF ISO/CEI 27000 FÉVRIER 2011 s’appliquent au 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 toutes les pièces ce rapportant au présent marché et à son exécution.

1. Confidentialité

Une information confidentielle désigne toute information de quelque nature (y inclus la méthodologie, la documentation, les informations ou le savoir-faire), sous quelque forme que ce soit (y inclus sous forme orale, écrite, magnétique ou électronique), sur tout support dont le CHU de Rouen est propriétaire ou titulaire, et qui est communiquée au Titulaire, ou obtenue de toute autre façon par ce dernier dans le cadre de ses relations avec le CHU de Rouen.

Le Titulaire qui, soit avant la notification du marché, 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.

Le Titulaire et son personnel, et le cas échéant ses sous-traitants, ne peut utiliser les informations confidentielles que pour l’accomplissement des prestations prévues au contrat. Toutefois, n’est pas considérée confidentielle toute information :

* qui était dans le domaine public au moment de sa divulgation ou que le CHU de Rouen aurait lui-même rendue publique pendant l’exécution du contrat ;
* signalée comme présentant un caractère non confidentiel et relative aux prestations du contrat ;
* qui a été communiquée au Titulaire par un tiers ayant légalement le droit de diffuser cette information, comme le prouvent des documents existant antérieurement à sa divulgation par le CHU de Rouen.

L’obligation de confidentialité s’étend aux données intéressant les patients et les personnels du CHU de Rouen dont le Titulaire, pourrait avoir connaissance dans le cadre de l’exécution du présent marché.

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 Titulaire 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 Titulaire 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 du CHU de Rouen, toutes conséquences de droit, en cas de divulgation des informations confidentielles par ses salariés, ses sous-traitants et leurs salariés.

Le Titulaire comme le CHU de Rouen 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 le CHU de Rouen et/ou par le Titulaire, 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 Titulaire vers les tiers, à l’exception des Sociétés Affiliées et sous-traitants du Titulaire, concernant le marché et son exécution doit être préalablement soumise à l’accord du CHU de Rouen.

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

Le Titulaire veille à ce qu'au cours de l'exécution du marché, soient respectées la sécurité et la confidentialité des Données et des accès informatiques du CHU de Rouen 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 Titulaire s’engage à ne pas conduire le CHU de Rouen à méconnaître ces dispositions, en procédant à toutes les préconisations utiles en ce sens.

Le Titulaire 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 du CHU de Rouen, à l’exception des Sociétés Affiliées et sous-traitants du Titulaire, aucune partie ou totalité d’un programme, d’un fichier et/ou d’une donnée détenu(s) par le CHU de Rouen 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 le CHU de Rouen e, et/ou aucune documentation détenue par le CHU de Rouen, à prendre toute mesure, notamment de sécurité matérielle pour assurer la conservation des supports tout au long de la durée du présent marché.

Les informations sensibles et celles de niveau Diffusion Restreinte doivent être protégées conformément à l’instruction interministérielle n° 901 relative à la protection des systèmes d’information sensibles. En cas de manipulation d’informations classifiées de défense, le Titulaire respecte l’instruction générale interministérielle n°1300 sur la protection du secret de la défense.

Le non-respect de ces dispositions décrit dans ce chapitre sur la Confidentialité pourrait entraîner la résiliation du contrat par le CHU de Rouen.

1. Sécurité

Le Titulaire et ses sous-traitants ultérieurs sont tenus de respecter les prescriptions de la politique générale de sécurité des systèmes d’information (PGSSI) du CHU de Rouen 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 Titulaire sur demande.

Les annexes techniques des procédures et modes opératoires sont rendues accessibles sur demande motivée.

Dans tous les cas, le Titulaire 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.

Afin de démontrer de manière économique la réalité de ses efforts pour sécuriser les composants et prestations impliqués dans le marché, le Titulaire communique les labels et certificats dont il est titulaire.

1. Directive NIS

Le Titulaire atteste avoir pris connaissance de la possible qualification en système d’information essentiel (SIE) du Progiciel ou des matériels associés par le CHU de Rouen au cours de l’exécution du marché conformément au 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 CHU de Rouen informe le Titulaire de cette qualification.

Le Titulaire 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 Titulaire informe le CHU de Rouen des conséquences sur l’exécution des prestations et fournitures.

Le Titulaire et le CHU de Rouen peuvent convenir d’un avenant au marché afin d’adapter les conditions d’exécution des prestations et fournitures.

1. Certification hébergeur de données de santé du CHU de Rouen

Le Titulaire atteste avoir pris connaissance de la possible intégration du Progiciel ou des matériels dans le périmètre des prestations rendues par le CHU de Rouen à ses clients et Partenaire relevant de la certification à l’hébergeur de données de santé au cours de l’exécution du marché 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.

Le CHU de Rouen informe le Titulaire de cette intégration.

Le Titulaire 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 Titulaire informe le CHU de Rouen des conséquences sur l’exécution des prestations et fournitures.

Le Titulaire et le CHU de Rouen peuvent convenir d’un avenant au marché afin d’adapter les conditions d’exécution des prestations et fournitures.

1. Accès physiques aux locaux

Le CHU de Rouen assure au personnel du Titulaire appelé à intervenir dans ses locaux, des conditions d’environnement conformes aux normes d’hygiène et de sécurité.

Le CHU de Rouen informe le Titulaire des consignes de sécurité dans lesdits locaux.

L’accès aux locaux du CHU de Rouen par le Titulaire est soumis aux règlements intérieurs imposés aux personnes extérieures du CHU de Rouen.

Le CHU de Rouen s'engage à limiter l’accès à l'ensemble de ses installations informatiques et télécoms et à mettre en place une procédure interne permettant de s'assurer qu'aucune personne étrangère au service et non autorisée ne peut accéder au local où sont hébergées les informations traitées dans le cadre du présent marché.

Le CHU de Rouen tient à jour un registre nominatif des personnels du Titulaire autorisés à intervenir dans ses locaux. Seuls les personnels du Titulaire 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 au CHU de Rouen. Ils s’engagent à les garder secrets, à ne pas les dévoiler ou les laisser à la disposition des tiers.

Au cours de ses visites dans les locaux du CHU de Rouen, le personnel du Titulaire ne peut être accompagné d’un tiers sans accord écrit préalable du CHU de Rouen ou du responsable du site concerné.

Aucune sortie des locaux du CHU de Rouen 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 le CHU de Rouen ne peut être faite sans l’autorisation préalable et écrite du CHU de Rouen.

Dans le cas des opérations de maintenance (par exemple, réparation matérielle), le Titulaire doit transmettre au préalable au CHU de Rouen un descriptif précisant les dates, la nature des opérations à effectuer et les noms des intervenants.

Le CHU de Rouen veille à la présence effective de l’un de ses préposés 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 du CHU de Rouen, à défaut du Titulaire, 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 Titulaire s’engagent à :

* Respecter les directives et procédures de sécurité du CHU de Rouen
* Informer sans délai le CHU de Rouen de tout départ, changement de fonction de ses préposés
* A ne pas tenter de contourner les procédures mises en œuvre par le CHU de Rouen permettant le contrôle des accès autorisés et empêchant les accès non autorisés à ses locaux
* Ne pas essayer de s’introduire dans des salles non autorisées ou avec d’autres moyens que ceux mis à sa disposition
* Ne pas permettre l’accès aux personnes non autorisées par le CHU de Rouen dans ses locaux
* Respecter les systèmes de sécurité physique mis en place au CHU de Rouen, 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 le CHU de Rouen permettant l’accès physique aux locaux du CHU de Rouen 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.

1. Vidéoprotection

Afin d’assurer la sécurité des biens ou des personnes, certains sites ou lieux sensibles du CHU de Rouen ont été équipés de système de vidéoprotection. Le Titulaire reconnaît être informé que de tels systèmes sont mis en place dans les sites sensibles. Le Titulaire et ses sous-traitants ultérieurs informent leurs préposés de la mise en œuvre de ces traitements par le CHU de Rouen. Le CHU de Rouen s’engage à respecter la législation applicable à ce type d’équipement.

1. Mesures liées aux réseaux

Le CHU dispose de nombreux réseaux de différents niveaux de confidentialité, notamment, par ordre de plus grande confidentialité :

* Réseaux serveurs et d’administration LAN ;
* Réseaux clients internes LAN ;
* DMZ privée ;
* DMZ publique.

Les solutions et matériels supportent une infrastructure multi-vlan / multi-réseaux, avec routage et filtrage par pare-feux en cœur de réseau.

Le Titulaire positionne les différentes ressources composant la solution sur les réseaux du bon niveau de confidentialité. Les flux d’échanges entre ces différentes ressources se font du réseau de plus haut niveau de confidentialité vers les réseaux de plus faible niveau.

Aucune ressource publiée sur Internet ne peut être située sur un LAN interne.

Les clients (postes de travail) peuvent accéder aux ressources dans les réseaux LAN, Serveurs et DMZ. Exemples :

* frontal web en DMZ publique ;
* base de données web en DMZ privée ;
* serveur interne sur LAN Serveur), etc.

Les postes de travail disposent d’un accès filtré à Internet (liste noire, filtrage applicatif, etc.).

Le Titulaire fournit la documentation des flux réseaux de son progiciel et/ou de ces matériels, c’est-à-dire a minima les informations suivantes : IP source, IP destination, ports, protocoles, mais aussi le type d’application.

Les règles de pare-feux mises en œuvre par le CHU sont strictes. Seuls les ports, destinations et applications strictement nécessaires seront ouverts (aucun champ « ANY » ne sera utilisé).

L’usage de protocoles fiables et non vulnérables est demandé, de préférence en TCP pour contrôler l’intégrité des transferts. Les protocoles SMB/CIFS notamment, ne sont pas recommandés s’ils ne sont pas à destination d’un serveur de fichier central du CHU.

Le Titulaire configure la solution selon les informations fournies par le CHU concernant le plan d’adressage et les adresses IP. Un système ne peut être relié à deux réseaux simultanément.

Les serveurs ne disposent pas d’un accès à Internet. Des sites web peuvent être autorisés au cas par cas de façon exceptionnelle (HTTPS uniquement) et sur justification de l’usage.

Les serveurs peuvent être autorisés à communiquer avec un serveur au travers d’Internet, sur justification. Le protocole utilisé est chiffré (transport). Les destinations sont définies (domaine, IP).

L’ouverture d’un portail ou d’un service sur Internet nécessite un certain nombre de mesures :

* Chiffrement obligatoire via l’usage de TLS 1.1, 1.2 ou supérieur ;
* Les flux réseaux passent au travers d’une sonde IDS/IPS et d’un antivirus de flux ;
* Les portails sont situés derrière un pare-feu, dans une DMZ publique ;
* Les ports depuis ou vers Internet sont strictement filtrés ;
* Aucun flux ne remonte dans les réseaux LAN.

1. Connexion du matériel du Titulaire sur les réseaux du CHU de Rouen

Dans le cas où le Titulaire aurait besoin, pour l’exécution de sa prestation, de connecter des matériels informatiques lui appartenant sur le réseau du CHU de Rouen, le Titulaire s’engage à :

* Recueillir préalablement l’accord express du CHU de Rouen
* Respecter les directives et procédures de sécurité du CHU de Rouen
* Ne pas entraver ou de contourner la mise en œuvre et l’action de l'ensemble des dispositifs de sécurité du CHU de Rouen.
* Garantir que son matériel ne présente aucun risque de compromission ou d’infection par un code informatique malfaisant, du réseau informatique du CHU de Rouen notamment par une analyse préalable avec un antivirus à jour avant chaque connexion au système d’information du CHU de Rouen
* 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 du CHU de Rouen
* 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, etc.) :
  + 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 Titulaire, le Titulaire utilise des postes de travail informatiques dédiées à l'exploitation et l'administration isolées des réseaux bureautiques, d'Internet, de la messagerie notamment. Si les actes sont réalisés depuis les locaux du CHU de Rouen, les postes de travail informatiques sont fournis par le CHU de Rouen.

1. Connexion au système d’information du CHU de Rouen par le Titulaire

Le Titulaire s’engage à respecter le volet Utilisateur de la Charte du bon usage du numérique annexée au règlement intérieur du CHU de Rouen, les directives et procédures de gestion des accès au système d’information du CHU de Rouen. Notamment :

* Respecter les directives et procédures de sécurité du CHU de Rouen
* Informer sans délai le CHU de Rouen de tout départ, changement de fonction de ses préposés
* A ne pas tenter d’entraver ou de contourner les procédures mises en œuvre par le CHU de Rouen 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
* Signaler tout défaut de sécurité ou situation qui semblerait anormale.

Le Titulaire est responsable de la gestion et de la confidentialité de ses moyens d’authentification, nécessaires accéder au système d’information du CHU de Rouen. Le Titulaire s’assure notamment que ses préposés ont connaissance et respectent les règles de l’art permettant de préserver la confidentialité des moyens d’authentification.

Le Titulaire supporte seul les conséquences pouvant résulter de la perte, la divulgation, ou l’utilisation frauduleuse ou illicite des moyens d’authentification fournis à ses préposés, la responsabilité du CHU de Rouen ne pouvant en aucun cas être engagée à ce titre.

Le Titulaire s’engage à informer le CHU de Rouen 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 la santé publique et afin de garantir la confidentialité des données de santé à caractère personnel et leur protection, le CHU de Rouen met à disposition du Titulaire 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.

1. Cartographie des systèmes d’information

En fonction de l’objet du marché, des enjeux financiers, de la complexité, et de la sensibilité des données, il est recommandé que le Titulaire s’inspire des préconisations issues du guide « Cartographie des systèmes d’information » de l’ANSSI.

Le Titulaire doit donc être en capacité de disposer d’un inventaire et d’une cartographie des systèmes d’information dont il a la charge et doit les maintenir, selon les préconisations de l’ANSSI, dans l’outil mis à sa disposition par le CHU de Rouen.

L’inventaire et la cartographie comprennent également la liste des « briques » matérielles et logicielles utilisées, ainsi que leurs versions exactes avec leur configuration. Ils comportent une base de données de configuration.

La cartographie est livrée à la demande du CHU de Rouen et selon une périodicité à valider au début du marché.

1. Echanges et communications d’informations

L’usage de la messagerie entre le Titulaire et le CHU de Rouen se limite à des échanges non confidentiels. Notamment, tout document du projet ne peut pas être transmis par messagerie électronique.

Le Titulaire et le CHU de Rouen s’engagent à utiliser la plateforme d’échange de fichiers <https://sirrus.chu-rouen.fr> pour échanger des documents.

Le Titulaire et le CHU de Rouen s’engagent à limiter l’usage des supports amovibles et à privilégier la plateforme d’échange de fichiers <https://sirrus.chu-rouen.fr>.

1. Protection contre les logiciels malveillants

Le Progiciel doit s’intégrer dans la stratégie antivirale du CHU de Rouen.

Les produits antivirus et antimalware du CHU (EDR et NGAV Cybereason pour les serveurs, EDR Cybereason et EndPoint Protection de Microsoft pour les postes de travail) sont installés sur tous les systèmes d’exploitation sans distinction.

Les exclusions éventuelles se font sur les processus. L’exclusion de dossiers ne représente pas l’état de l’art et doit être évitée, bien qu’elle reste possible sur justification forte et transmise en amont de l’installation. Aucune exclusion n’est possible sur les dossiers partagés (ex : dossier Windows\Temp).

1. Gestion des vulnérabilités

Le Titulaire réduit au maximum la surface d’attaque de sa solution et de ses matériels. Seuls les services et applications strictement nécessaires sont installés et utilisés.

Le CHU de Rouen procède à une recherche périodique des vulnérabilités techniques de son système d’information. Elle utilise le référentiel Common Vulnerability Scoring System (CVSS) en version 2.0 du National Institute of Standards and Technology (NIST), et notamment le guide de mise en œuvre « CVSS Implementation GUIDANCE » pour caractériser les vulnérabilités techniques.

Le Titulaire s’engage à contribuer à la gestion des vulnérabilités de ses fournitures et prestations en apportant son soutien le CHU de Rouen.

Sont considérées comme Vulnérabilité critique, les vulnérabilités techniques des fournitures et prestations du Titulaire, qui ont les caractéristiques suivantes :

1. Vecteur d’attaque (ACCESS VECTOR) = Réseau (NETWORK)

2. Complexité d’exploitation (ACCESS COMPLEXITY) inférieure ou égale à moyen (MEDIUM)

3. Authentification = non nécessaire (NONE)

4. Impact sur la confidentialité, l’intégrité ou la disponibilité supérieure ou égale à partiel (PARTIAL).

Sont considérées comme vulnérabilité majeure, les vulnérabilités techniques des fournitures et prestations du Titulaire, qui ont les caractéristiques suivantes :

1. Vecteur d’attaque (ACCESS VECTOR) = réseau adjacent (ADJACENT NETWORK) ;

2. Quelle que soit la complexité d’exploitation ;

3. Avec ou sans authentification ;

4. Impact sur la confidentialité, l’intégrité ou la disponibilité supérieure ou égale à partiel (PARTIAL).

Les autres vulnérabilités techniques des fournitures et prestations du Titulaire sont considérées comme vulnérabilité mineure.

Leur résolution suit les règles de gestion des incidents telles que définies dans le présent marché.

Le CHU de Rouen met en œuvre un plan de maintenance préventive des composants technologiques sous-jacent aux prestations du Titulaire (Systèmes d’exploitation, base de données, etc.) en appliquant périodiquement les correctifs de sécurité publiés par leur éditeur respectif ou communauté. Nota : *Dans le cadre du présent marché, la mise en œuvre du plan de maintenance peut être délégué au Titulaire*.

La période de mise à jour par défaut est le trimestre excepté, pour les vulnérabilités critiques qui doivent être comblées sans délai (correctif de sécurité ou mesure d’atténuation) et planifiées en accord avec le CHU de Rouen.

Le Titulaire garantit la bonne exécution de ses prestations dans le cadre de ce plan de maintenance. Tout dysfonctionnement des fournitures et prestations du Titulaire qui résulterait de la mise en œuvre du plan de maintenance est imputable au Titulaire. Leur résolution suit alors les règles de gestion des incidents définies dans le présent marché.

Le Titulaire doit n’utiliser que des composants logiciels que l’éditeur s’engage à maintenir pendant la durée du marché. Si la durée du marché dépasse la durée pendant laquelle un éditeur s’engage à maintenir un composant logiciel, le Titulaire maintient, livre et respecte une feuille de route de migration vers des systèmes maintenus.

Le Titulaire ne peut conditionner ses garanties de bon fonctionnement de fournitures ou prestations à l'emploi de composants dans une version non supportée par leur éditeur respectif et ou la communauté Open Source, sauf à démontrer une contrainte supérieure et proposer à ses frais des moyens de cantonner les risques, ou démontrer que les risques sont négligeables dans le contexte d'emploi.

Le Titulaire s’assure que l’application des correctifs de sécurité ne modifie pas les performances du système, en modifiant si besoin et à ses frais le système pour maintenir le niveau de performance malgré l’application du correctif.

1. Signalements de sécurité

Le Titulaire met à disposition des fils publics par abonnement (flux RSS, liste de diffusion par courriel) ou autre dispositif d'information dédié à la sécurité informatique. Ces fils, identifiés en début de contrat et communiqués par mail auprès de la boite [DSI.RSSI@chu-rouen.fr](mailto:DSI.RSSI@chu-rouen.fr), permettent au CHU de Rouen d'être tenu informés en continu des événements et changements impactant la sécurité.

Afin de garder leur pouvoir d'alerte, ces canaux de diffusion ne sont pas mélangés avec des flux commerciaux et marketing.

Le Titulaire a obligation d'enregistrer les failles auprès des autorités compétentes notamment le CERT-FR en suivant les réglementations établies. A défaut d'action sous 3 mois, le CHU de Rouen a la possibilité de se substituer au Titulaire 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).

Le Titulaire est tenu à une obligation permanente de conseil et de mise en garde, relative aux matériels, logiciels et prestations fournies au CHU de Rouen. Dans ce cadre, le Titulaire notifie au CHU de Rouen toute information permettant d’améliorer le niveau de sécurité du système d’information et signaler les difficultés et risques que certains choix peuvent entraîner. Dans l'hypothèse où le Titulaire ne respecte pas cette obligation, il ne peut se prévaloir d'une incohérence dans le marché pour s'exonérer de ses obligations contractuelles.

1. Télémaintenance

La maintenance à distance n’est possible que s’il existe un lien contractuel entre le prestataire et le CHU.

Dans le cas où le Titulaire réalise une prestation de maintenance sur des ressources du CHU de Rouen ou celles du Titulaire installées sur le réseau du CHU de Rouen, le Titulaire s’engage à respecter les règles suivantes :

* Respecter les directives et procédures de sécurité du CHU de Rouen ;
* A ne pas tenter de contourner les procédures mises en œuvre par le CHU de Rouen 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 ;
* Utiliser le bastion d’administration du CHU de Rouen tout autre accès étant interdit ;
* Obtenir l'accord préalable du CHU de Rouen avant chaque opération ;
* Transmettre systématiquement à le CHU de Rouen 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 malfaisant, du réseau informatique du CHU de Rouen ;
* Traiter les moyens d’authentification comme des informations confidentielles ;
* Télé-assister les utilisateurs ou les personnels du CHU de Rouen chargés de la mise en œuvre du système d’information conformément aux recommandations de la commission nationale de l’informatique et des libertés (CNIL) depuis les outils mis à disposition par le CHU de Rouen.

L’accès pour la prise en main à distance sur des ressources installées sur le réseau du CHU se fait uniquement au travers d’un VPN SSL fourni par le CHU.

Les protocoles autorisés au travers du bastion d’administration / proxy d’authentification sont : RDP et SSH uniquement.

Le prestataire n’a pas le droit de mettre en œuvre d’autres moyens de prise en main à distance que ceux fournis par le CHU (Remote Viewer). Teamviewer, AmmyyAdmin, VNC et autres logiciels de prise en main à distance sont interdits.

Les agents du Titulaire sont responsables du compte qui leur est fourni. Ils ne doivent pas divulguer les identifiants, et être en en capacité permanente de savoir qui a utilisé le compte à un moment donné.

1. Téléservices de l’administration électronique

Si les prestations ou fournitures du Titulaire sont destinées à être le support de téléservice, voire offrir des téléservices, entrant dans le champ de l’ordonnance 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives (Cf. Décret 2010-112 du 2 février 2010 et l’arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité), le CHU de Rouen procède à l’homologation de sécurité du téléservice au plus tard en phase de Vérification d’Aptitude (VA).

1. Homologation de sécurité

Le CHU de Rouen met en œuvre une démarche d’intégration de la sécurité dans les projets et procède à une homologation de sécurité ses applications et services conformément au Référentiel Général de Sécurité (RGS). Le Titulaire s’engage apporter son concours en matière de documentations et de réponses aux questions, permettant d'analyser les risques résiduels en matière de confidentialité, authentification, traçabilité, intégrité, disponibilité et résilience.

Le Titulaire assiste le CHU de Rouen dans l’élaboration des procédures et modes opératoire suivants :

* La description exhaustive (technique et fonctionnelle) du Progiciel et/ou des matériels mis en œuvre
* La description de la gestion des profils, comptes et habilitations (procédure de gestion des comptes d’accès, modèle d’habilitation et la procédure de gestion des habilitations, etc.)
* Une documentation d’exploitation décrivant les opérations de maintien en condition opérationnelle :
  + Procédures sécurisées d’arrêt et redémarrage des serveurs et matériels,
  + Procédures de sauvegarde des systèmes et de données,
  + Procédure de restauration,
  + Prérequis de supervision,
  + Mécanismes de haute disponibilité,
  + Mécanismes de vérification d’intégrité,
  + etc.
* Les procédures de contrôles des installations logiciels (cahier de tests techniques/fonctionnels, etc.)

1. Personnel du Titulaire

Le Titulaire a obligation de transmettre au CHU de Rouen la liste des personnes contribuant à l'exécution de la prestation, ainsi que les engagements de reconnaissance de responsabilité signés (joint en annexe). En cas de sous-traitance, l’agrément du sous-traitant doit inclure l’engagement de reconnaissance de responsabilité signé par le sous-traitant en accompagnement de l’agrément du sous-traitant.

Le Titulaire sensibilise son personnel, intervenant dans le cadre des prestations, à la sécurité de l’information, des systèmes d’information et aux règles du CHU de Rouen. Le Titulaire veille notamment à ce que son personnel intervenant dans le cadre de des prestations respecte les dispositions concernant la sécurité du présent marché.

En cas de départ définitif d’une personne nommément désignée, affectée par le Titulaire à l’exécution des prestations du marché, le titulaire doit :

* en aviser, sans délai, le CHU de Rouen et prendre toutes dispositions nécessaires, afin d’assurer la poursuite de l’exécution des prestations ;
* proposer au CHU de Rouen un remplaçant disposant de compétences au moins équivalentes et dont il lui communique le nom, les titres dans un délai d’un mois à compter de la date d’envoi de l’avis mentionné à l'alinéa précédent.
* Le remplaçant proposé par le Titulaire est considéré comme accepté par le CHU de Rouen, si celui-ci ne le récuse pas dans le délai d’un mois courant à compter de la réception de la communication mentionnée ci-dessus.
* Si l’acheteur récuse le remplaçant, le Titulaire dispose d’un mois pour proposer un autre remplaçant.
* La décision de récusation prise par le CHU de Rouen est motivée.

En aucun cas le remplacement du personnel ne peut justifier une augmentation des prix du marché. Pendant toute la durée d’exécution des prestations visées au présent marché, le CHU de Rouen se réserve le droit de récuser les membres du personnel qui s’avéreraient inadaptés à l’exécution des prestations sur la base des résultats correspondant à une période d’essai d’un mois. Il motive sa décision après concertation avec le Titulaire. Ce dernier procède au remplacement du personnel récusé dans les conditions précisées ci-dessus.

1. Les exigences fonctionnelles de sécurité pour un progiciel
2. Identification/Authentification

La composante privée du Progiciel 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 réussies.

Lorsqu’elles sont nécessaires, l'identification et l'authentification entre l’utilisateur et le Progiciel doivent être réalisées au sein d’un environnement sûr. Pour chaque interaction, le Progiciel 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 Progiciel. 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 Progiciel 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.

1. Contrôle d’accès

Le Progiciel 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 Progiciel.

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 Progiciel, le Progiciel doit vérifier la validité de la demande. Les tentatives d'accès non autorisés doivent être rejetées.

1. Journalisation / imputabilité

Le Progiciel 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 Progiciel 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 Progiciel. Toute action sur une donnée d’imputation devra être tracée

1. Protection de l’intégrité du Progiciel

En standard, l’intégrité du Progiciel est assurée par les moyens de contrôle d’intégrité des bases de données et des serveurs mis en place systématiquement par le CHU de Rouen.

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 Progiciel 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.

1. Prestations d’achat de matériels/logiciels

Le CHU de Rouen s’assurera une vigilance particulière lors de l’acquisition ou la location de matériels/logiciels sur les points suivants :

* Absence de failles à la mise en production : le Titulaire s’engage à ce que les produits du contrat soient, au jour de leur mise en production pour le CHU de Rouen, dépourvus de toute faille, faiblesse ou défaut de conception portant atteinte à la sécurité des informations.
* Détection d’une vulnérabilité : en cas de mise en évidence d’une vulnérabilité affectant un produit du contrat, le Titulaire doit mettre à disposition du CHU de Rouen dans les meilleurs délais une solution de contournement ou une solution palliative (mise à disposition de correctifs) n’affectant ni les performances ni les fonctionnalités du produit concerné. Le Titulaire collabore également avec le CHU de Rouen pour déterminer l’origine de la vulnérabilité et les actions à engager pour l’éradiquer.
* Exigences liées à la maintenance : dans le cadre d’une opération de maintenance, le Titulaire s’engage à chiffrer ou effacer de manière sécurisée toutes les données avant l’envoi en maintenance externe de toute ressource informatique de l’acheteur. Si les données ne sont pas sensibles, et si elles ne peuvent être chiffrées ou effacées en totalité (par exemple : disque dur défectueux sous garantie), l’envoi en maintenance externe ne peut se faire que sous couvert d’un engagement de confidentialité de la part du mainteneur, ou bien dans le cadre d’une réparation sur site en présence d’un membre de l’équipe locale chargée des systèmes d’information. Si les données sont sensibles et si elles ne peuvent être chiffrées ou effacées en totalité, l’envoi en maintenance externe est interdit.
* Exigences liées à la télémaintenance : dans le cadre d’un accès de télémaintenance à une ressource informatique (matériel, logiciel) de l’acheteur, le titulaire doit présenter des mesures de sécurité renforcées validées par le CHU de Rouen ;
* Mise au rebut : pour tout départ définitif d’un matériel ou logiciel du service, le Titulaire doit empêcher de manière sécurisée l’accès aux données présentes sur les disques durs ou dans la mémoire intégrée. Un procès-verbal doit être signé entre le titulaire et l’acheteur. En cas d’impossibilité de réaliser un effacement sécurisé sur tout ou partie des disques ou de la mémoire (par exemple pour raison de panne ou dysfonctionnement), le disque dur ou la mémoire doit être détruit(e) physiquement avant de quitter définitivement le service ou démonté(e) et entreposé(e) sur site dans un local sécurisé en attente de destruction.

1. Hébergement des données et des services

En fonction de la sensibilité des données ou des services qui seront confiés au Titulaire, le CHU de Rouen demandera des précisions sur la localisation et l’hébergement des données ou des services liés à la prestation.

Le Titulaire précisera dans un Plan d’Assurance Sécurité transmis au CHU de Rouen les lieux géographiques dans lesquels :

* Les données informatiques liées à la prestation seront hébergées ;
* Les services objets de la prestation seront localisés ;
* Les systèmes d'accès et d'administration des services liés à la prestation seront localisés.

De même, le Titulaire indique si ses infrastructures (techniques ou organisationnelles) sont gérées ou simplement accessibles par une entité juridique appartenant à un pays disposant de lois autorisant ce pays à accéder aux données.

Le Titulaire décrit le cas échéant les risques de sécurité environnementaux dont font l’objet les sites hébergeant les données ou du service et précise dans un plan de prévention des risques (PPR) les mesures mises en œuvre pour couvrir ces risques.

1. Réversibilité, Transférabilité et Destruction des Données

En fin de marché ou en cas de résiliation, le Titulaire doit prémunir le CHU de Rouen contre toute interruption ou baisse de la qualité des services avant la fin dudit marché.

Dans le cas où un Plan d’Assurance Sécurité est demandé, cette phase de transfert devra être décrite par le Titulaire dans ce document. Sinon l’acheteur doit prévoir les modalités de transfert dans son offre. Le Titulaire assure également l’ensemble des opérations pour que le CHU de Rouen puisse reprendre les services dans de bonnes conditions (transfert de compétences, documentations, etc.).

Le Titulaire met en œuvre des mesures techniques et organisationnelles pour garantir la sécurité des données et des applications qui lui sont confiées, notamment s’il est prévu un transfert de prestations de la part du précédent Titulaire en conformité avec les réglementations applicables.

Durant la phase de transfert, l’assurance de la sécurité réside notamment dans :

* La gestion des accès, habilitations ;
* Le transfert de responsabilités ;
* La fourniture d’informations nécessitant des mesures de protection adaptées ;
* La gestion de la continuité de l’activité.

Au terme du marché ou en cas de résiliation, le Titulaire restitue sans délai au CHU de Rouen une copie de l’intégralité des données confiées par lui dans le cadre de la prestation. Une fois la restitution effectuée, le Titulaire doit détruire, dans un délai de trois mois, les éventuelles copies de données détenues dans son système d’information, y compris les données ayant fait l’objet de sauvegardes ou d’un archivage.

La restitution et la destruction des données seront constatées par un procès-verbal daté et signé par le Titulaire. Les procédés de destruction sont conformes aux réglementations en vigueur (instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale, instruction interministérielle N°901 relative aux mesures de protection des systèmes d’information traitant d’informations sensibles non-classifiées de défense de niveau Diffusion Restreinte).

1. Méthodologie sécurisée d’ingénierie et de développement

Le Titulaire met en œuvre une méthodologie spécifique pour les prestations intégrant de l’ingénierie ou encore de développement sécurisée pour un Progiciel.

Le Titulaire décrit dans sa réponse les 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.

1. Obligations spécifiques liées aux prestations d’étude

Le Titulaire doit respecter les standards et les méthodologies préconisés au sein du CHU de Rouen. En particulier, le Titulaire doit appliquer les méthodes d’évaluation de la sensibilité et d’analyse de risques des systèmes d’information lorsqu’il intervient dans les phases amont des projets.

Le Titulaire doit utiliser différents environnements cloisonnés pour les activités de développement, de recette et de pré-production.

Lors de la conduite de tests de validation ou du déploiement, le Titulaire doit :

* utiliser des données de tests anonymisées (sauf accord explicite du CHU de Rouen) ;
* ne pas provoquer de perturbations du système d’information du CHU de Rouen lors des séances de test ;
* remettre en l’état initial les systèmes testés et réinitialiser le matériel sensible.

1. Obligations spécifiques liées aux prestations de développement

Le Titulaire doit utiliser le cadre commun de développement (méthodes, démarches, etc.) du CHU de Rouen comprenant notamment :

* l’organisation des équipes de développement et de la prestation ;
* les configurations matérielles préconisées pour le développement ;
* les outils de développement préconisés par le CHU de Rouen (logiciels, versions, etc.) ;
* une structure de développement (framework) intégrant les fonctions de sécurité.

Le CHU de Rouen est propriétaire du code et des droits de propriété intellectuelle des éléments développés dans le cadre de la prestation.

Le Titulaire doit utiliser différents environnements cloisonnés pour les activités de développement, de recette et de pré-production.

Le Titulaire doit mettre en œuvre les mesures de sécurité nécessaires et adéquates à la protection des codes sources.

Le titulaire doit commenter et documenter le code développé dans le cadre de la prestation. La documentation doit être mise à jour régulièrement.

Toute activité de développement doit être tracée et conservée dans un format facilitant son exploitation ultérieure.

Le titulaire doit sauvegarder et conserver chaque version du code source recettée dans le cadre de la prestation. Les accès à ces sauvegardes devront être tracés.

Le titulaire doit déposer les codes sources dans ses différentes versions et mises à jour selon les recommandations du CHU de Rouen.

Lors de la conduite de tests de validation ou du déploiement, le titulaire doit :

* utiliser des données de tests anonymisées ;
* ne pas provoquer de perturbations du système d’information de l’acheteur lors des séances de test ;
* remettre en l’état initial les systèmes testés et réinitialiser le matériel sensible ;
* ne pas introduire de régression vis-à-vis d’un état de sécurité atteint dans une version précédente

Le CHU de Rouen se réserve le droit de contrôler la qualité et la sécurité du développement fourni par le Titulaire, via des audits et/ou des tests d’intrusion par exemple (audit de code sur les parties les plus sensibles, etc.).

1. Etats de l'art

La sécurisation des systèmes informatiques dépend de l'évolution des technologies. Il appartient au Titulaire de s'aligner sur les standards et référentiels qui concernent les services qu'il propose, utilise, met à disposition ou exploite.

Le Titulaire garantit au CHU de Rouen qu’il est conforme à l’état de l’art pour les services et objets numériques fournis dans le cadre des prestations.

Pour les interfaces web, les services de courriels, les appareils connectés, les sauvegardes de données et les consoles d'administration de systèmes d'information, les référentiels à retenir sont résumés ci-après et détaillés dans les textes techniques publiés sur le site de l’ANSSI <https://www.ssi.gouv.fr/administration/bonnes-pratiques/>.

A la première demande, le candidat ou titulaire fournit la conformité à ces référentiels pour les services et objets numériques qu'il inclut dans son offre de fournitures. Il précise alors les domaines concernés (interfaces web et courriels), les objets et bases d'information concernées (appareils connectés, sauvegardes de données, consoles d'administration).

1. Interfaces web

* Les interfaces web sont utilisables par des navigateurs à l'état de l'art (part de marché cumulée supérieure à 50%), sans générer d'alerte de sécurité ;
* Les développements ne doivent pas générer d'adhérence avec des modules spécifiques (Flash, Silverlight, JRE, etc.), une technologie en particulier ou en lien avec un module d'extension d’un navigateur web ;
* Les mécanismes cryptographiques TLS (https) doivent être systématiquement activés pour identifier et authentifier la source et protéger les communications. L'utilisation de la technologie HSTS est fortement recommandée ;
* Les mécanismes de protection des cookies de session (HttpOnly, Secure, SameSite) sont mis en œuvre pour se protéger des vols ou exploitation de sessions déjà ouvertes ;
* Une politique de sécurité des contenus (CSP, SRI) et des navigateurs (emploi d’entêtes de sécurité (X-Content-Type-Options, X-Frame-Options, X-XSS-Protection, Referrer-Policy) est élaborée pour se protéger contre les injections de contenus actifs malicieux ;
* Les obligations légales sont renseignées sur les sites Internet et un point de contact est publié via le fichier /.well-known/security.txt pour permettre des signalements directement auprès des points de contact technique identifiés ;

1. Services de courriels

* L’authenticité des émetteurs est garantie par l'émission de messages depuis des serveurs associés publiquement aux domaines, signature numérique par domaine et une politique publique liant le tout ;
* L’intégrité des messages est vérifiable par leur signature numérique ;
* Les mécanismes de chiffrement TLS sont notamment mis en œuvre pour l'authentification, la lecture et la distribution des messages (STARTTLS, SMTPS, IMAPS, etc.) ;
* La mise en œuvre des mécanismes permettant de garantir l'authenticité des émetteurs est systématiquement envisagée (contrôle des noms de domaines associés aux serveurs (SPF), signature numérique (DKIM), politique de sécurité liant le tout (DMARC)) ;
* L’identification claire du statut des comptes émetteurs de courriels, par exemple en ajoutant un suffixe à ceux fournis aux personnels qui ne sont pas agents ou salariés directs, est demandée ;
* Confidentialité des échanges de machines en machines, confidentialité compatible avec les obligations d'interceptions légales ;
* Analyse des rapports d'anomalies via DMARC ou abuse@.

1. Composants techniques

Seuls les systèmes dont la date de fin de support n’est pas dépassée sont autorisés. Ci-dessous une liste non exhaustive de composants concernés :

* Microsoft Windows pour les postes de travail : 7, 10
* Microsoft Windows pour les serveurs : 2012 et supérieur.
* Environnement Linux pour les serveurs : RedHat Enterprise, Centos, etc.
* Base de données : Oracle, SQL Server, MySQL, etc.

Les systèmes d’exploitation doivent être supportés par l’éditeur pour une durée d’au moins 3 ans après la date de réception de la solution ou prévoir la migration en cours du marché sans surcoût.

Les systèmes d’exploitation peuvent également être mis à jour par le CHU de façon automatique, sans validation préalable.

Les solutions du Titulaire sont virtualisées, sauf indication contraire dans le CCTP, besoin de performance particulier (exemple : PACS, GRID de calcul), ou nécessité d’être physique (machine-outil, appliance). Le socle technique est une plateforme de virtualisation VMware. Les VMTools seront installés sur les machines. Un hébergement sur une plateforme de virtualisation de type Hyper-V est également possible.

Quel que soit le type d’hébergement sur le système d’information du CHU de Rouen, des livrables seront demandés par le CHU de Rouen auprès du Titulaire pour expliciter l’architecture de la solution.

Les horloges des ressources sont synchronisées sur un serveur de temps que le CHU met à disposition.

Le CHU applique ses politiques de sécurité (GPO, utilitaires, etc.) sur les composants techniques intégrés dans le domaine, notamment une politique de mot de passe. Il est recommandé que le Progiciel s’intègre dans le domaine Active Directory de l’établissement et supporte les groupes AD pour la gestion des droits. Le Progiciel ne fait pas de copie locale de la base AD.

1. Appareils connectés

* Dispositif de lutte contre les logiciels malveillants (anti-virus, ou système de vérification et détection à base de signatures ou condensats des logiciels autorisés).
* Dispositif de mise à jour sécurisé.
* Limitation de l'exposition via les réseaux en réduisant les ports acceptant des connexions entrantes et en authentifiant les accès distants, sans faille connue (ceci exclut les connections non chiffrés Telnet, HTTP/SMTP sans TLS, et l'emploi de mots de passe génériques ou faciles à découvrir, par exemple du fait d'un hachage insuffisant).

1. Sauvegardes des données stockées

Le CHU dispose d’un outil de sauvegarde.

L’ensemble des serveurs et des données sont sauvegardés, les besoins en sauvegarde étant définis selon la criticité des ressources et d’après une politique interne de sauvegarde. Le Titulaire apporte son support pour un fonctionnement adéquat de la sauvegarde. Le Titulaire décrira les recommandations de sauvegarde et de restauration au travers d’une Documentation d’Exploitation fournie auprès du CHU de Rouen.

L’architecture technique du Progiciel est compatible avec un système de sauvegarde des machines virtuelles si elle est hébergée sur une plateforme de virtualisation (VMWare ou Hyper-V).

La politique de sauvegardes du CHU de Rouen vise à tendre vers la règle du 3-2-1 (3 copies, 2 technologies, 1 exemplaire hors site principal, donc avec chiffrement) pour se protéger des rançongiciels, des erreurs de manipulations ou des défaillances de matériels. La stratégie de sauvegarde doit s'inscrire dans le cadre de la réflexion globale de gestion du système d'information et être intégrée au Plan de Continuité et de Reprise de l'Activité (PRA/PCA).

1. Administration des systèmes d'information

* Consoles dédiées à l'exploitation et l'administration, et à minima isolées des réseaux bureautiques et d'Internet, web et courriel notamment.
* Connexions aux machines administrées par des protocoles chiffrés, authentifiants et sans faille connue et bien configurés (VPN IPsec, TLS, ssh, RDP avec NLA).
* Il est fortement recommandé de ne pas créer de dossiers partagés directement sur les ressources constituant la solution. Le CHU dispose de serveurs de fichiers centralisés et sauvegardés pour ce besoin. Les dossiers partagés nécessaires disposent de droits appropriés : droits NTFS par groupes Active Directory, limités en droits (au maximum : modification), et limités en nombre de personnes (comptes nominatifs uniquement).
* Les composants techniques et la solution dispose de droits « administrateur local » pour la durée de l’installation. Lorsque l’installation est terminée, les droits « administrateur local » sont retirés. Lorsque la solution nécessite des droits sur l’Active Directory, un compte de service est mis en œuvre. Il ne dispose que des droits strictement nécessaires au fonctionnement de la solution. Aucune solution ne disposera de droits « administrateur du domaine ».
* Les mots de passe des comptes par défauts (exemples : root, admin, invité, administrateur, etc.) sont modifiés et respectent la politique de mots de passe du CHU. Aucun mot de passe n’est codé en dur. Les comptes génériques ne sont pas autorisés pour s’assurer d’une utilisation strictement interdite dès lors qu’il y a un accès à des données d’un haut niveau de confidentialité (de santé notamment).

1. Audit

Le CHU de Rouen peut effectuer ou de faire effectuer un audit de sécurité auprès du Titulaire ou le cas échéant de ses sous-traitants afin de s’assurer de la prise en compte effective du niveau de sécurité requis par l’acheteur.

Le Titulaire se soumet aux questionnaires ou audits de sécurité que le CHU pourrait lui demander. Le CHU prend en charge le coût direct de l’audit : auditeurs, déplacements et frais des auditeurs. L’objectif de l’audit est de s’assurer que le Titulaire respecte ses obligations en termes de sécurité.

Le Titulaire est informé 15 jours à l’avance (date de l’audit, modalités financières pour l’acheteur et le titulaire, etc.).

Le CHU de Rouen, ou l’organisme mandaté à cette fin, peut, pendant une période de six mois à compter de la fin ou de la résiliation du marché, exercer un contrôle dans les locaux du titulaire et, le cas échéant, dans ceux de ses sous-traitants afin de vérifier que les dispositions en matière de destruction des données ont été effectivement appliquées.

En cas de non-conformité au niveau d’exigence de sécurité requis par le CHU de Rouen, un plan de remédiation devra être formalisé par le Titulaire 15 jours après la constatation des écarts. Le Titulaire doit ensuite régulariser ces écarts par l’application du plan de remédiation dans un délai convenu en commun accord entre les deux parties.

Le Titulaire effectue des autocontrôles de conformité aux exigences de Sécurité pour garantir le niveau de sécurité au démarrage de la prestation ainsi que son maintien tout au long de la prestation. Ceux-ci sont décrits dans un Plan d’Assurance Sécurité transmis auprès du CHU de Rouen.

Afin de répondre à des opérations d’audits et de certifications (Certification des Comptes, Certification Hôpital Numérique, Certification Haute Autorité de Santé, COFRAC, etc.), il doit également exister des outils pour examiner les fichiers d'imputation. Ces outils doivent être documentés. Ils doivent notamment permettre d'identifier sélectivement les actions d'un ou de plusieurs utilisateurs sur les solutions et matériels mis en place par le Titulaire dans le cadre du présent marché.

1. Annexes
2. 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 surmontés avec de réelles difficultés | Conséquences significatives voire irrémédiables non surmontables |
| **Impact sur le CHU de Rouen** | | | | | |
| **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 du CHU de Rouen en interne | Dégrader temporairement l'image du CHU de Rouen au niveau régional | Dégrader temporairement la réputation du CHU de Rouen au niveau national | Dégrader durablement la réputation du CHU de Rouen au niveau national | Dégrader durablement la réputation du CHU de Rouen au niveau mondial |
| Juridique | Absence de réclamation | Réclamation non contentieuse | Risque de réclamation indemnitaire | Réclamation indemnitaire ou risque de réclamation pénale | Réclamation pénale |

1. Documents de référence

Ci-dessous, une liste non exhaustive des documents de référence dans le cadre du marché/contrat :

* **Données classifiées :**
* Instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale
* Instruction interministérielle n°901/SGDSN/ANSSI du 28 janvier 2015
* **Réglementations spécifiques à la protection de certains systèmes d’information :**
* Instruction interministérielle n°901/SGDSN/ANSSI du 28 janvier 2015 relative aux mesures de protection des systèmes d’information traitant d’informations sensibles non-classifiées de défense de niveau Diffusion Restreinte (DR), informations dont la divulgation à des personnes non autorisées, l'altération ou l'indisponibilité sont de nature à porter atteinte à la réalisation des objectifs des acheteurs qui les détiennent.
* Référentiel général de sécurité (RGS) dans sa version en vigueur
* Articles L. 1332-6-1 et L. 1332-6-3 du code de la défense qui peuvent imposer l’utilisation de produits et de services (audit, détection) qualifiés
* **Référentiels pour le secteur Santé**
* Politique de Sécurité des Systèmes d’Information de l’Etat (PSSI-E) : Circulaire du Premier Ministre n°5725/SG (NOR : PRMX1420095C) du 17 juillet 2014
* Corpus documentaire de la Politique Générale de Sécurité des Systèmes d’Information de Santé (PGSSI-S) et les guides complémentaires de l’ASIP Santé
* Politique de Sécurité des Systèmes d’Information pour les ministères chargés des affaires sociales (PSSI-MCAS)
* Exigences de sécurité prévues par le Programme Hôpital Numérique (instruction N°DGOS/MSIOS/2012/376 du 31 octobre 2012).
* Exigences de sécurité prévues par la Certification HAS (Haute Autorité de Santé)
* Exigences de sécurité prévues dans l’Auditabilité des SIH dans le cadre de la Certification des Comptes (instruction N°DGOS/MSIOS/2013/62 du 21 février 2013).
* **Référentiels de l’ANSSI :**
* Les guides de l’Agence Nationale de la Sécurité des Systèmes d’Information dont les guides d’hygiène informatique, de bonnes pratiques et celui sur l’administration sécurisée constituent un socle fortement recommandé.
* **Données à caractère médical :**
* Article L. 1111-8 du code de la santé publique sur l’hébergement des données de santé
* Référentiel de Certification Hébergeur de Données de Santé - Exigences et contrôles
* **Données de recherche, données stratégiques et techniques :**
* Décret n° 2011-1425 du 2 novembre 2011 portant application de l'article 413-7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation, arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation
* **Données à caractère personnel :**
* Règlement (UE) 2016/679 du parlement européen et 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) dit RGPD
* **Directive Network and Information Security (NIS) :**
* Directive NIS (Network and Information System Security) (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concerne la mise en œuvre de mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information au sein de l'Union Européenne.
* **Normes :**
* NF ISO/CEI 27000
* NF ISO/CEI 9001
* **Documents internes :**
* Politique de Sécurité du Système d’Information simplifiée de l’établissement
* Dossier d’homologation d’un système d’information