Référentiel Sécurité des Systèmes d’Information de Santé

|  |  |  |  |
| --- | --- | --- | --- |
| Approbation du document | | | |
| **Nom** | **Fonction** | **Date** | **Visa** |
| F. Alliaume | RSSI | 25/10/2018 |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |
| --- |
| MISE EN œuvre ET REVISION DU DOCUMENT |
| Le Responsable de la Sécurité des Systèmes d’Information (RSSI) de l’établissement est en charge de la diffusion, de la mise à jour et de la révision du document. |

|  |  |  |  |
| --- | --- | --- | --- |
| Historique du document | | | |
| **Version** | **Date** | **Nom** | **Actions** |
| 1.0 | 5/9/2018 | F. Alliaume/E.Guillou | Création du document |
| 1.1 | 25/10/2018 | F. Alliaume | Prise en compte remarques C. Roy |
| 2 | 30/04/2019 | E. Guillou | Prise en compte des remarques de la cellule juridique des contrats |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Sommaire

[1 Introduction 4](#_Toc7512167)

[2 Exigences GENERALES sur les logiciels et leur installation 5](#_Toc7512168)

[3 Identités 8](#_Toc7512169)

[4 Authentification 9](#_Toc7512170)

[5 Tracabilité 10](#_Toc7512171)

[6 Protection des systèmes 12](#_Toc7512172)

[7 Cryptographie 13](#_Toc7512173)

[8 Maintenance et Télémaintenance 14](#_Toc7512174)

[9 Specifications wi-fi 18](#_Toc7512175)

[10 Protection des donnees medicales 18](#_Toc7512176)

[11 CAS PARTICULIERS SELON PERIMETRE 19](#_Toc7512177)

[12 Glossaire des termes employés 24](#_Toc7512178)

# Introduction

Les solutions informatiques déployées au sein du Système d’Information du CHU de Rennes doivent :

* Satisfaire les exigences de sécurité informatique définies dans la politique cadre de sécurité du CHU de Rennes ;
* Respecter les préconisations en matière de sécurité de l’ASIP, 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.**

Les **recommandations sont des orientations techniques** fortement souhaitées en matière de sécurité pour apporter une cohérence avec les bonnes pratiques et recommandations du secteur santé. Elles sont notées **R comme Recommandé**.

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.

Les présentes exigences de sécurité sont intégrées dans le marché public conclu avec le CHU de Rennes et s’imposent 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.

# Exigences GENERALES sur les logiciels et leur installation

| **Ref.** |  | **Règle de sécurité** | **Description de la prise en charge** | **Evaluation par le CHU de Rennes** |
| --- | --- | --- | --- | --- |
| 2.1 | **O** | 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. |  |  |
| *2.2* | ***O*** | Pour tout ce qui est fourni au titre de l’offre, le titulaire s’engage à acquérir et à céder au CHU de Rennes 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…). |  |  |
| 2.3 | **O** | Le titulaire s’engage à n’installer et n’activer que les seuls logiciels nécessaires au bon fonctionnement du dispositif objet du marché. |  |  |
| 2.4 | **O** | Pour les logiciels libres, la conformité du logiciel est de la responsabilité du titulaire seul. Ils devront aussi respecter les exigences de sécurité. |  |  |
| 2.5 | **O** | Pour les logiciels gratuits, la conformité du logiciel est de la responsabilité du titulaire seul : ils devront aussi respecter les exigences de sécurité. |  |  |
| 2.6 | **O** | 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. |  |  |
| 2.7 | **O** | Les personnels du titulaire devront respecter la Charte applicable aux prestataires accédant au Système d’Information de l’établissement lors de toute intervention à l’installation ou en maintenance. Le titulaire s’engage à en informer ses personnels. |  |  |
| 2.8 | **O** | 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. |  |  |
| 2.9 | **R** | Les systèmes ou logiciels s’appuyant sur une fonctionnalité d’*Auto-logon* ne sont pas souhaités hors cas particulier à décrire. |  |  |
| 2.10 | **R** | Lorsque des données à caractère personnel sont gérées par l’application, le titulaire fournit une procédure ou un outil d’anonymisation pour pouvoir être appliqué à tout autre environnement que celui de production. |  |  |
| 2.11 | **R** | Les applications ou services nécessitant un fonctionnement permanent, seront hébergés sur des machines ayant un système d’exploitation de type serveur et ne seront pas dépendantes d’une session utilisateur (fonctionnement en mode service). |  |  |
| 2.12 | **R** | Seules des versions de système d’exploitation supportées et maintenues par l’éditeur en termes de mise à jour de sécurité seront installées.  Le titulaire décrira tous les cas particuliers nécessitant une protection supplémentaire. |  |  |
| 2.13 | **O** | Si la solution proposée doit être hébergée sur un serveur de l’établissement, elle doit s’intégrer dans l’environnement technique de la Direction du Système d’Information décrit dans le Cahier des charges. |  |  |
| 2.14 | **R** | Si la solution proposée comporte des objets connectés (IOT), un rapport d’audit de sécurité par un organisme spécialisé indépendant du titulaire est souhaité avec la réponse. |  |  |
| 2.15 | **O** | 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. |  |  |

# Identités

LE CHU DE Rennes a choisi le service d’annuaire de la société Microsoft (AD : Active Directory) comme référentiel des comptes utilisateurs.

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Evaluation**  **Par le CHU de Rennes** |
| --- | --- | --- | --- | --- |
| 3.1 | **R** | L’exploitation de cet annuaire comme source d’identité logicielle est souhaité et peut revêtir deux formes :   * Déport de la gestion d’identité de l’application au sein de l’annuaire du CHU de Rennes. * Mise à disposition d’un point d’entrée (web service, connecteur…) permettant au CHU de Rennes de synchroniser le référentiel d'identités de l’application avec son référentiel d’identité et d’authentification (IAM).   En l’absence de ces modes, il convient de décrire la gestion des identités au sein de son dispositif. |  |  |

# Authentification

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Evaluation**  **Par le CHU de Rennes** |
| --- | --- | --- | --- | --- |
| 4.1 | **R** | Il est souhaitable que les systèmes et applications supportent les mots de passe complexes et la définition de stratégies. |  |  |
| 4.2 | **O** | Les mots de passe des comptes nécessaires à l’administration de la solution doivent pouvoir être modifiés par le CHU de Rennes. |  |  |
| 4.3 | **O** | Pour les applications web exposées sur internet et qui intègreraient une authentification et/ou une gestion des comptes :  Les pages réservées à l’authentification et à la création de comptes doivent intégrer un dispositif de protection contre l’usage de robots.  Des mécanismes empêchant de réutiliser des informations de connexion ou de session pour contourner l’authentification doivent être en place. |  |  |
| 4.4 | **O** | Pour les applications web exposées sur internet et qui intègreraient une authentification et/ou une gestion des comptes, les mécanismes d’authentification doivent être adaptés à la criticité des données.  Une authentification forte par carte CPS ou équivalent est exigée pour l’accès à des données de santé (sauf disposition contraire du Cahier des charges qui conduirait le CHU de Rennes 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). |  |  |
| 4.5 | **R** | Pour les applications web un audit externe de sécurité de type top 10 de l’OWASP est souhaité avec l’offre. |  |  |
| 4.6 | **R** | Si une gestion des habilitations est mise en œuvre, elle doit s’intégrer dans l’environnement technique du CHU de Rennes décrit dans le Cahier des charges. |  |  |

# Tracabilité

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Evaluation** |
| --- | --- | --- | --- | --- |
| 5.1 | **R** | Il est souhaitable que la solution proposée conserve de manière sécurisée ses éléments de traçabilité. |  |  |

Contenu de la trace :

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Evaluation** |
| --- | --- | --- | --- | --- |
| 5.2 | **O** | La capacité à tracer toutes les actions (y compris la consultation de données) doit être décrite. |  |  |
| 5.3 | **O** | Les accès utilisateurs (et administrateurs) seront tracés en réussite et en échec. |  |  |
| 5.4 | **O** | Dans le cadre de systèmes gérant des données à caractère personnel, les traces de consultation et de modification sont obligatoires. |  |  |
| 5.5 | **O** | Les traces produites devront être accessibles par un outil de centralisation des traces 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). |  |  |
| 5.6 | **R** | S’agissant des modifications de valeurs sensibles au sein du dispositif, il est souhaité que les traces correspondantes comportent la valeur en amont et en aval de l’événement. La suppression d’une donnée du point de vue applicatif ne saurait engendrer la perte de l’historique des accès et modifications associées à cette donnée. |  |  |
| 5.7 | **R** | Lorsque la gestion des autorisations applicatives – même partiellement – est du ressort de l’application, il est souhaitable que tout événement relatif à l’édition d’un profil ou d’un utilisateur soit tracé. |  |  |
| 5.8 | **R** | Dans le cas d’architectures N-Tiers ou lors de l’usage de comptes applicatifs, il est souhaitable que les traces comportent l’utilisateur d’origine et l’ordinateur source de la connexion. Si cela s’avérait impossible, il serait souhaitable que la mise en corrélation des traces des différentes strates applicatives par le biais des identifiants de session puisse permettre de déterminer avec certitude la continuité de l’accès. |  |  |

# Protection des systèmes

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Evaluation** |
| --- | --- | --- | --- | --- |
| 6.1 | **O** | Le titulaire doit s’engager à ce que la solution installée respecte le niveau de sécurité requis par le CHU de Rennes pour assurer le maintien en conditions de sécurité de son Système d’Information.  Ses dispositifs doivent soit :   * s’intégrer dans la démarche de sécurité du CHU de Rennes en installant l’antivirus du CHU de Rennes et en inscrivant ses systèmes dans les règles de gestion des correctifs de sécurité en vigueur pour le reste du SI. * minimiser les risques inhérents à la nature des composants de la solution. Ceci implique de maintenir à niveau en termes de sécurité les composants qui pourraient présenter des risques, en garantissant une administration sécurisée intégrant au moins une solution de protection contre les codes malveillants tenue à jour (antivirus ou protection équivalente) et un système d’exploitation ainsi que tous les composants mis à jour des correctifs de sécurité publiés par les éditeurs selon des modalités et une fréquence à décrire. * proposer un système d’étanchéité de la solution par rapport au Système d’Information (pare-feu). Dans ce cas, le titulaire fournira tous les moyens nécessaires au CHU de Rennes pour s’assurer de la bonne étanchéité de la solution, en particulier un compte d’accès en lecture aux règles de filtrage du pare-feu.   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. |  |  |

# Cryptographie

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Evaluation** |
| --- | --- | --- | --- | --- |
| 7.1 | **O** | 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 SSL fournis par le CHU de Rennes depuis son autorité de certification interne. |  |  |
| 7.2 | **O** | Les données utiles à l’authentification doivent être chiffrées lors de leur communication et de leur stockage. |  |  |
| 7.3 | **O** | De manière générale, si des techniques cryptographiques sont utilisées, elles doivent être conformes aux standards du marché, et au Référentiel Général de Sécurité (RGS). |  |  |

# Maintenance et Télémaintenance

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** |
| --- | --- | --- | --- | --- |
| 8.1 | **O** | Pour ce qui concerne les besoins d’accès distants en supervision sur des dispositifs maintenus, l’envoi d’informations vers un site distant doit être décrit précisément en indiquant toutes les données transférées ou consultées. L’usage exclusif à des fins de maintien en conditions opérationnelles doit être garanti ainsi que l’absence de transfert de données à caractère personnelles.  Cette remontée d’information devra utiliser des protocoles sécurisés, être tracée et passer par les passerelles de contrôle d’accès à internet du CHU de Rennes ou par un tunnel VPN avec le site de télédiagnostic.  La solution mise en œuvre devra assurer la protection des accès et des données, la traçabilité, la preuve opposable et la possibilité d’audit par le CHU de Rennes. |  |  |
| 8.2 | **O** | Pour les besoins de télémaintenance seule, la connexion doit se faire via la passerelle Internet sécurisée mise à disposition par le CHU de Rennes (VPN SSL ou VPN IPSEC). |  |  |
| 8.3 | **O** | Au niveau des postes de travail standard du CHU de Rennes, aucun outil de prise de contrôle à distance ne peut être installé dans le cadre de la maintenance d’une application sans l’accord préalable et écrit du CHU de Rennes. |  |  |
| 8.4 | **O** | Il est de la responsabilité du titulaire d’assurer la sécurité de sa plateforme d’intervention à distance (données et logiciels). |  |  |
| 8.5 | **O** | LE CHU DE Rennes 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. |  |  |
| 8.6 | **O** | Le titulaire doit avoir une politique anti-virus et de mise à jour des correctifs de sécurité appliquée sur les postes de télémaintenance. |  |  |
| 8.7 | **R** | Il est souhaitable que les postes de télémaintenance soient isolés physiquement du réseau local du titulaire. |  |  |
| 8.8 | **O** | Les données à caractère personnel ou technique du CHU de Rennes (configuration des équipements) exploitées par les équipes de support chez le titulaire ne doivent pas être divulguées (une protection adaptée doit être réalisée). |  |  |
| 8.9 | **O** | L’intervention de maintenance est encadrée par le présent marché public entre le CHU de Rennes et le titulaire, définissant les engagements de chacun, les modalités pratiques, … |  |  |
| 8.10 | **O** | Le titulaire s’engage sur la sécurité de la prestation. Son représentant devra signer la Charte applicable aux prestataires qui accèdent au Système d’Information du CHU de Rennes rappelant la confidentialité des données et l’engageant à informer ses personnels que tous les accès et actions seront tracés. |  |  |
| 8.11 | **O** | 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). |  |  |
| 8.12 | **O** | Il est de la responsabilité du titulaire de connaitre en toutes circonstances l’identité de toute personne qui se connecte ou qui s’est connectée sur la plateforme de télémaintenance et d’en assurer la traçabilité (cette traçabilité sera communiquée au CHU de Rennes sur simple demande de celui-ci). |  |  |
| 8.13 | **O** | 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 (fichiers exécutables, fichiers temporaires, documentation, etc). |  |  |
| 8.14 | **O** | Le titulaire réalise un suivi permanent des incidents et vulnérabilités liés aux dispositifs connectés et met à disposition les correctifs nécessaires. |  |  |
| 8.15 | **O** | 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. |  |  |
| 8.16 | **O** | Le titulaire garantit la mise à niveau de sa solution en cas d’obsolescence du système d’exploitation.  Il en est de même pour tous les autres logiciels indispensables au bon fonctionnement de la solution.  A défaut il fournira sans surcoût les moyens pour maintenir un niveau de sécurité suffisant (dispositif de sécurité complémentaire, pare-feu…). |  |  |
| 8.17 | **O** | Le titulaire doit fournir un rapport détaillé de l’intervention effectuée. |  |  |
| 8.18 | **O** | Pour les besoins de télémaintenance seule, si le CHU de Rennes dispose d’un 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 pourra être ouvert et fermé par le CHU de Rennes à la demande du titulaire (mainteneur) ou de la personne habilitée selon le protocole défini dans les conditions de la maintenance. |  |  |
| 8.19 | **R** | Le titulaire pourra établir un PAS (Plan Assurance Sécurité) afin de faire connaitre les dispositions de sécurité qu’il met en place pour sa prestation. Le PAS traite :   * Des critères de sécurités utilisés dans la désignation des personnes chargées des interventions. * De la désignation des sites d’exécution de la prestation, protection et accès physiques des locaux utilisés. * Des règles de protections des informations du Système d’Information associées à la prestation de télémaintenance. * De l’architecture générale de la plateforme d’intervention (cloisonnement technique etc.). * Des accès logiques à la plateforme, identification et authentification, mise en veille, déconnexion automatique, gestion des droits, traçabilité… * Des dispositions prises pour assurer la continuité de l’activité après un sinistre ou un incident majeur. * De l’assurance et des contrôles de la sécurité des services de l’intervention fournis. |  |  |

# Specifications wi-fi

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Evaluation** |
| --- | --- | --- | --- | --- |
| 9.1 | **O** | Le chiffrement et l’intégrité des informations circulant sur les réseaux sans-fil doivent être assurés par la mise en place sur les équipements concernés des protocoles garantissant le plus haut niveau de sécurité (version WPA2 minimum définie dans la norme IEEE 802.11i certifiée par la Wifi Alliance). |  |  |
| 9.2 | **R** | Pour l’authentification, l’association avec un serveur d'authentification 802.1X (Radius) est recommandée. Pour éviter la gestion redondante des comptes, le serveur devra s’appuyer sur l’annuaire LDAP centralisé de l’établissement. Pour des équipements spécifiques qui seraient incompatibles avec ce paramétrage, une description des niveaux possibles et des compléments de sécurisation doivent être fournis pour évaluation d’un mode de prise en charge de la sécurité acceptable. |  |  |

# Protection des donnees medicales

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Evaluation** |
| --- | --- | --- | --- | --- |
| 10.1 | **O** | Le titulaire et son personnel 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. |  |  |

**Article L1110-4 du Code de la Santé Publique**

Toute personne prise en charge par un professionnel de santé, un établissement ou service, un professionnel ou organisme concourant à la prévention ou aux soins dont les conditions d'exercice ou les activités sont régies par le présent code, le service de santé des armées, un professionnel du secteur médico-social ou social ou un établissement ou service social et médico-social mentionné au I de l'article [L. 312-1](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006074069&idArticle=LEGIARTI000006797382&dateTexte=&categorieLien=cid) du code de l'action sociale et des familles a droit au respect de sa vie privée et du secret des informations la concernant.

Excepté dans les cas de dérogation expressément prévus par la loi, ce secret couvre l'ensemble des informations concernant la personne venues à la connaissance du professionnel, 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 tous les professionnels intervenant dans le système de santé.

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Evaluation** |
| --- | --- | --- | --- | --- |
| 10.2 | **O** | En conséquence, notamment, les jeux de données fournies par le CHU de Rennes sont strictement confidentiels et sont liés au secret professionnel. |  |  |
| 10.3 | **R** | Un outil de chiffrement des données est souhaité. Cet outil doit permettre de protéger les informations de la base de données ou bien des fichiers de données pour préserver le secret médical. |  |  |
| 10.4 | **R** | En outre, il est souhaitable que cet outil préserve l’anonymat des personnes dans le cas de données de tests. |  |  |

# CAS PARTICULIERS SELON PERIMETRE

* Cas de moyens mobiles :

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Evaluation** |
| --- | --- | --- | --- | --- |
| 11.1 | **R** | Il est souhaitable que les dispositifs mobiles portables (clés USB, ordinateurs portables) soient chiffrés et les clefs de chiffrement remises au CHU de Rennes. |  |  |

* Cas de service hébergé en dehors du Système d’information du CHU de Rennes (pour **tout ou partie de l’objet du marché)** et cas de services administrés en autonomie par le titulaire (SaaS)

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Evaluation** |
| --- | --- | --- | --- | --- |
| 11.2 | **O** | 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 (PSSIE) et du ministère de la santé (PSSI-MCAS).  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 du pays concerné. |  |  |
| 11.3 | **O** | 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’ASIP (ou toute commission compétente désignée par la réglementation). |  |  |
| 11.4 | **O** | 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 *les clauses de conformité au RGPD.* |  |  |
| 11.5 | **O** | Si des données nominatives à caractère personnel font l’objet de traitement par le système, une conformité au RGPD est nécessaire et le titulaire devra démontrer le niveau de protection adapté à la criticité de ces données. Cette démonstration doit être intégrée dans les descriptions de la prise en charge des mesures concernées du présent document, en accord avec *les clauses de conformité au RGPD* annexées au contrat. |  |  |

* **Concernant l’accès au service hébergé par des utilisateurs du CHU de Rennes :**

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Evaluation** |
| --- | --- | --- | --- | --- |
| 11.6 | **O** | 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). |  |  |
| 11.7 | **O** | Les mots de passe ne doivent pas être stockés en clair dans le logiciel ou la base de données. Ils ne doivent pas non plus être stockés de manière réversible dans la base de données ou le logiciel (sauf cas particuliers validés par le CHU de Rennes) |  |  |
| 11.8 | **O** | Le titulaire doit remettre un compte et authentifiant pour audit au RSSI du CHU de Rennes et accepte que le CHU de Rennes réalise ou commandite des audits externes pour vérifier la conformité aux exigences de sécurité. |  |  |

* **Concernant la continuité du service hébergé :**

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Evaluation** |
| --- | --- | --- | --- | --- |
| 11.10 | **O** | Le fournisseur précisera les durées d’indisponibilité sur lesquelles il s’engage. Le service ne doit pas être indisponible plus que la durée décrite dans le marché. |  |  |
| 11.11 | **R** | Il est souhaitable qu’une copie exploitable des données (fichier informatique avec champs délimités et décrits, base de donnée si accord du CHU de Rennes) soit transmise ou accessible régulièrement. Le fournisseur indiquera le délai possible.. Il décrira le mode de mise à disposition.  Lors de leur transmission, la protection des données sera impérativement assurée avec le même niveau de sécurité que celui appliqué à leur stockage et à leur accès chez le titulaire (chiffrement, authentification…). |  |  |

* **Concernant la réversibilité du service hébergé :**

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Evaluation** |
| --- | --- | --- | --- | --- |
| 11.12 | **O** | Une copie exploitable des données (base de données ou fichier informatique avec champs délimités et décrits) est transmise au CHU de Rennes 3 mois avant la fin du marché public pour permettre la réalisation de tests de migration. Le mode de mise à disposition sera décrit par le fournisseur. |  |  |
| 11.13 | **O** | Une copie exploitable des données (base de données ou fichier informatique avec champs délimités et décrits) est transmise au CHU de Rennes en fin de contrat. Le mode de mise à disposition sera décrit par le fournisseur.  Lors de leur transmission, la protection des données doit impérativement être assurée avec le même niveau de sécurité que celui appliqué à leur stockage et à leur accès chez le titulaire (chiffrement, authentification…). |  |  |

* **Concernant la garantie de Confidentialité des données hébergées :**

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Evaluation** |
| --- | --- | --- | --- | --- |
| 11.14 | **O** | Le titulaire s’engage à garantir un accès aux données aux seules personnes habilitées selon les besoins du CHU de Rennes. |  |  |
| 11.15 | **R** | Il est souhaitable que les intervenants du titulaire qui peuvent avoir accès aux données soient identifiés et signent la Charte applicable aux prestataires accédant au Système d’Information de l’établissement. Les accès et actions réalisées devront être tracés. |  |  |
| 11.16 | **O** | Le titulaire s’engage à détruire les données en fin de contrat après les avoir restituées au CHU de Rennes sous une forme exploitable. |  |  |

* **Règles supplémentaires si la solution est installée dans l’infrastructure informatique du CHU de Rennes mais administrée intégralement par le titulaire :**

| Ref. |  | **Règle de sécurité** | **Description de la prise en charge** | **Evaluation** |
| --- | --- | --- | --- | --- |
| 11.17 | **O** | L’accès depuis l’extérieur du CHU de Rennes pour l’exploitation et la maintenance doivent respecter les conditions décrites au paragraphe Maintenance et Télémaintenance du présent document. |  |  |
| 11.18 | **O** | Pour tout type de traitement le titulaire doit remettre un compte et authentifiant pour audit au RSSI du CHU de Rennes et accepte que le CHU de Rennes réalise ou commandite des audits externes pour vérifier la conformité aux exigences de sécurité. |  |  |
| 11.19 | **O** | Les échanges avec l’extérieur du CHU de Rennes doivent être sécurisés : utilisation de protocoles sécurisés et filtrage/contrôle par les équipements de sécurité du CHU de Rennes (le CHU de Rennes se réserve le droit de tracer tout accès et action sur les systèmes installés dans son infrastructure). |  |  |

# Glossaire des termes employés

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 extensible[[1]](https://fr.wikipedia.org/wiki/Extensible_Markup_Language#cite_note-2) » en français) est un métalangage informatique de balisage générique.

**L’organisme paraphe toutes les pages et signe ce document**

Fait à ………………… , le…/…/…

**Pour *l’organisme***

**(nom et qualité du signataire et cachet de l’organisme)**