Table des matières

[1 Préambule 3](#_Toc511994611)

[2 Exigences fonctionnelles de sécurité 3](#_Toc511994612)

[2.1 Démarche utilisée 3](#_Toc511994613)

[2.2 Définitions & référentiels 3](#_Toc511994614)

[2.2.1 Définitions 3](#_Toc511994615)

[2.2.2 Référentiels utilisés 5](#_Toc511994616)

[2.3 Exigences de sécurité du projet 7](#_Toc511994617)

[2.4 Synthèse 7](#_Toc511994618)

[3 Clauses de sécurité 8](#_Toc511994619)

[3.1 Obligations du titulaire 8](#_Toc511994620)

[3.2 Plan d’Assurance Sécurité (PAS) 8](#_Toc511994621)

[3.3 Localisation du service et des données 8](#_Toc511994622)

[3.4 Données personnelles – Informatique et Libertés 8](#_Toc511994623)

[3.4.1 Rôle des Parties (au sens des articles du RGPD (2016/679 du 27/04/2016) 8](#_Toc511994624)

[3.4.2 Caractéristiques du traitement de Données Personnelles 9](#_Toc511994625)

[3.4.3 Obligations des Parties concernant le Traitement de Données Personnelles 10](#_Toc511994626)

[3.4.4 Registres 12](#_Toc511994627)

[3.5 Données de santé à caractère personnel – Agrément hébergement données de santé 13](#_Toc511994628)

[3.6 Comité de suivi sécurité 13](#_Toc511994629)

[3.7 Qualité et niveaux de service 14](#_Toc511994630)

[3.8 Audits de sécurité et contrôles 15](#_Toc511994631)

[3.9 Application des plans gouvernementaux 15](#_Toc511994632)

[3.10 Sécurité dans les développements applicatifs 16](#_Toc511994633)

[3.11 Gestion des évolutions 16](#_Toc511994634)

[3.12 Réversibilité 16](#_Toc511994635)

[3.13 Restitution des données 18](#_Toc511994636)

[4 Exigences de sécurité 19](#_Toc511994637)

[4.1 Prévention d’une attaque ou d’un incident 19](#_Toc511994638)

[4.2 signalement des incidents graves de sécurité 19](#_Toc511994639)

[4.3 Sauvegardes 19](#_Toc511994640)

[4.4 Isolement et confinement 20](#_Toc511994641)

[4.5 Imputabilité, traçabilité 20](#_Toc511994642)

[4.6 Plan de secours 20](#_Toc511994643)

[4.7 Confidentialité et intégrité des flux 21](#_Toc511994644)

[4.8 Gestion des flux 21](#_Toc511994645)

[4.9 Authentification 22](#_Toc511994646)

[4.10 Sécurité des postes de travail 22](#_Toc511994647)

[4.11 Sécurité du site Internet accédé par le CHU d’Angers 22](#_Toc511994648)

[4.12 Gestion de la déconnexion 23](#_Toc511994649)

[4.13 Maintenance évolutive et information 23](#_Toc511994650)

[4.14 Suivi des contrats de maintenance tiers 23](#_Toc511994651)

[4.15 Charte fournisseur 23](#_Toc511994652)

# Préambule

La présente annexe liste les exigences de sécurité devant être satisfaite par le soumissionnaire.

Ceci afin de préserver le CHU d’Angers des dommages qu’il pourrait subir du fait de l’indisponibilité de ces ressources, d’une atteinte à leur intégrité ou à leur confidentialité, ou de l’incapacité à disposer des éléments de preuve des opérations qui leur sont associées.

Cette annexe est accompagnée :

* d’un bordereau de réponse « Bordereau de réponses - SSI - Mode hébergé avec données de santé.xlsx ».

Il est demandé au candidat de cocher avec justesse et précision les colonnes OFFRE et ETAT de REALISATION à droite des tableaux.

La colonne « Préférence Chu » indique si la réponse est :

1 – obligatoire

2 – souhaitée

3 – facultative

* d’un Plan d’Assurance Sécurité
* de clauses contractuelles de sous-traitance pour les fournisseurs du CHU d’Angers

# Exigences fonctionnelles de sécurité

## Démarche utilisée

Les exigences en termes de disponibilité, d’intégrité, de confidentialité et de preuve ont été analysées grâce à un tableau unique des enjeux de sécurité issu du GMSIH présenté ci-après. L’analyse se fait par activité ou fonctionnalité, en imaginant un ou plusieurs scénarios de risque et l’impact engendré en cas de dysfonctionnement. Elle aboutit à un tableau de synthèse des exigences souhaitées.

## Définitions & référentiels

### Définitions

Les exigences de sécurité sont exprimées sous forme de disponibilité, d’intégrité, de confidentialité et de preuve. Ces termes répondent aux définitions suivantes.

**Disponibilité :** Qualité d’une information d’être, à la demande, utilisable par une personne ou un système. Aptitude du système à remplir une fonction dans des conditions définies d’horaires, de délais et de performances.

**Intégrité :** Qualité d’une information de ne pouvoir être altérée, détruite ou perdue par accident ou malveillance.

**Confidentialité :** Qualité d’une information de n’être connue que par des personnes ayant besoin de la connaître.

Les notions de **preuve**, **contrôle**, **traçabilité** et **auditabilité** sont regroupées dans une définition commune : Garantir une maîtrise complète et permanente sur le système et en particulier pouvoir retracer tous les événements au cours d'une période définie.

###### 

### Référentiels utilisés

Les référentiels utilisés ci-dessous sont issus des études sur la sécurité du GMSIH.

#### Grille des impacts sécurité

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Axes d’impact** | **Seuils d’impact** | | | |
| 1  **limité** | 2  **important** | 3  **grave** | 4  **critique** |
| Atteinte à la qualité des soins | Perturbations momentanées et limitées de l’organisation des soins | Perturbations limitées dans la délivrance des soins | Désorganisation des soins ou atteinte limitée à l’état de santé d’un patient | Atteinte grave à l’état de santé d’un patient |
| Perturbation du fonctionnement interne | **Perturbation limitée** (< 1 semaine) d’un processus ne remettant pas en cause le respect d’un calendrier | **Perturbation significative**  (> 1 semaine)d’un ou plusieurs processus, ne remettant pas en cause leur viabilité ou un calendrier | **Désorganisation** **très importante**  (> 1 semaine)d’un ou plusieurs processus et, susceptible de remettre en cause leur viabilité ou un calendrier | **Désorganisation durable (plusieurs semaines) et non maîtrisée** d’un ou plusieurs processus **engageant gravement** la responsabilité du CHU d’Angers à l’égard du non-respect d’un calendrier |
| Pertes financières | Pertes non significatives sur le plan financier | Pertes < 1% du budget global ou du chiffre d’affaires | Pertes de l’ordre de 1% du budget global ou du chiffre d’affaires | Pertes > 1 %du budget global ou du chiffre d’affaires |
| Engagement de la responsabilité | Plainte(s) de patient(s) signalant un dysfonctionnement | Plainte(s) de patient(s) signalant un dysfonctionnement grave  ou débouchant sur un recours | Plainte(s) de patient(s) débouchant sur une sanction disciplinaire à l’encontre d’un responsable | Plainte(s) de patient(s) débouchant sur la condamnation civile ou pénale d’un responsable d’établissement |
| Atteinte à l’image de l’établissement (auprès des patients, partenaires, tutelles, médecins de ville,…) | Divulgation limitée d’incidents | Altération significative de l’image de l’établissement | Altération très importante de l’image de l’établissement | Altération définitive de l’image de l’établissement |

#### Grille des exigences de sécurité en fonction du niveau de risque

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **NIVEAU de risque** | **D-DISPONIBILITE** | **I-INTEGRITE** | **C-CONFIDENTIALITE** | **P-PREUVE & CONTROLE** |
| **1**  **COURANT** | **Interruption**  **= ou > à 1 semaine**  Indisponibilité des informations acceptée sans remise en cause du service fourni | **Signalement**  Perte d’intégrité momentanée d’informations acceptée et non remise en cause du service fourni | **Public**  Les informations peuvent être lues par tous | **Faible**  Les éléments d’auditabilité sont faibles et non immédiatement disponibles  (ex : journalisation d’accès) |
| **2**  **SENSIBLE** | **Interruption**  **< ou = 3 jours**  Indisponibilité tolérée sous réserve qu’elle soit momentanée, signalée et sans conséquence pour le service fourni | **Signalement et correction**  Perte tolérée si signalée et corrigée dans un délai suffisant pour ne pas avoir de conséquence grave sur le service fourni | **Restreint**  Les informations sont diffusées ou accessibles par des populations identifiées et contrôlables | **Auditable**  Les éléments de traçabilité des opérations existent et peuvent être rendus disponibles |
| **3**  **MAJEUR OU CRITIQUE** | **Interruption**  **< ou = 1 journée**  Les informations doivent toujours être fournies pour remplir le service attendu | **Justification a posteriori**  Les informations doivent rester intègres pendant la période d’utilisation ; toute perte en dehors de la période d’utilisation doit être signalée et corrigée ; si la perte d’intégrité est constatée pendant la période d’utilisation, le service ou traitement est arrêté jusqu’au rétablissement de l’intégrité | **Secret médical ou professionnel**  informations protégées (secret médical, secret professionnel) par la législation sur les données à caractère personnel et médical.  **Données nominatives**  **non médicales**  protégées par la législation sur la protection des données nominatives | **Preuve interne**  Fourniture d’une preuve opposable (mais contestable) |
| **4**  **STRATEGIQUE OU VITAL** | **Interruption**  **< ou = 4 heures**  Les informations doivent en permanence être accessibles et utilisables par tous les services concernés | **Certification a priori**  Les informations sont certifiées intègres pendant toute leur durée de vie ou leur période de validité | **Haute protection**  Secret médical renforcé  Exemple : informations dont la prise de connaissance non autorisée entraîne nécessairement un préjudice pour la personne concernée (ex : certaines pathologies) | **Preuve externe**  Fourniture d’une preuve incontestable |

## Exigences de sécurité du projet

La démarche présentée ci-dessus aboutie à la grille des exigences de sécurité couvrant l’ensemble des fonctions souhaitées. Elle montre la nécessité de mettre en place certains services de sécurité. Comme pour les référentiels précédents, le niveau de sécurité souhaité est exprimé grâce à Dn, In, Cn, Pn où « n » est un nombre compris entre 1 et 4.

Grille des exigences de sécurité

|  |  |  |
| --- | --- | --- |
| **SCENARIO DE RISQUE** | **IMPACT (justification)** | **Niveau de service souhaité**  **(classification)** |
| **Disponibilité** | Perturbation du fonctionnement interne  Perturbation momentanée et limitée de l’organisation des soins | Interruption < ou = à 3 jours **(D2)** |
| **Atteinte à la confidentialité** | Atteinte à l’image de l’établissement | Accès restreint à des populations identifiées et contrôlables **(C2)** |
| **Atteinte à l’intégrité des données** | Perturbation du fonctionnement interne | Les informations doivent rester intègres pendant la période d’utilisation ; toute perte en dehors de la période d’utilisation doit être signalée et corrigée ; si la perte d’intégrité est constatée pendant la période d’utilisation, le service ou traitement est arrêté jusqu’au rétablissement de l’intégrité **(I3)** |
| **Preuve et contrôle** | Incapacité à fournir des preuves en cas de besoin | Capacité à fournir des preuves incontestables **(P4)** |

## Synthèse

Le titulaire devra fournir des solutions fonctionnelles et techniques permettant de répondre aux exigences de sécurité suivantes :

|  |  |  |  |
| --- | --- | --- | --- |
| **Disponibilité** | **Intégrité** | **Confidentialité** | **Preuve et contrôle** |
| **D2** | **I3** | **C2** | **P4** |

# Clauses de sécurité

## Obligations du titulaire

Le titulaire est tenu à une obligation de conseil, de mise en garde et de recommandations en termes de sécurité et de mise à l’état de l’art. En particulier il s’engage à informer le CHU d’Angers des risques d’une opération envisagée, des incidents éventuels ou potentiels, et de la mise en œuvre éventuelle d’actions correctives ou de prévention.

Le titulaire est responsable du maintien en condition de sécurité du système pendant toute la durée du marché.

Les mécanismes de sécurité mis en œuvre doivent évoluer conformément à l’état de l’art : la découverte de failles dans un algorithme, un protocole, une implémentation logicielle ou matérielle, ou encore l’évolution des techniques de cryptanalyse et des capacités d’attaque par force brute doivent être prises en compte.

## Plan d’Assurance Sécurité (PAS)

Le Plan d’Assurance Sécurité annexé au présent marché, est à remplir par le titulaire. Il décrit l’ensemble des dispositions spécifiques que le titulaire s’engage à mettre en œuvre pour garantir le respect des exigences de sécurité du CHU d’Angers.

Le PAS est un document contractuel qui se substitue aux éventuelles clauses génériques de sécurité du titulaire.

## Localisation du service et des données

Le titulaire s’engage à satisfaire aux dispositions de la loi du 6 janvier 1978 modifiée, relative à la protection des données personnelles. A ce titre, il communiquera la liste de tous les lieux de stockage des données (site d’hébergement principal, site(s) de secours, lieu de stockage de sauvegarde, …).

## Données personnelles – Informatique et Libertés

Le titulaire pourra être amené à participer au traitement de données personnelles relatives à des patients et/ou au personnel administratif, médical ou paramédical de l’établissement. Le présent chapitre décrit les droits et obligations des parties, le cas échéant.

### Rôle des Parties (au sens des articles du RGPD (2016/679 du 27/04/2016)

* CHU ANGERS : «responsable du traitement»

Article 4.7 du RGPD : La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

Lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.

* Le TITULAIRE : «sous-traitant»

Article 4.8 du RGPD : La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement;

Le titulaire assure présenter les garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées pour assurer la sécurité des Données Personnelles et le respect des droits des Personnes Concernées.

### Caractéristiques du traitement de Données Personnelles

Mentions devant figurées dans la mission prévue au marché :

* L’intitulé, l’objet et les caractéristiques des traitements de Données Personnelles auxquels le titulaire est susceptible d’avoir accès (ci-après, le « *Traitement* »),
* les catégories de Personnes Concernées et de Données Personnelles traitées,
* la nature des prestations attendues du titulaire.

La liste des éléments inclus dans le Traitement est susceptible d’évoluer durant la mission prévue au marché.

Le titulaire reconnait et accepte que tout ou partie des Données Personnelles traitées par le CHU d’Angers constituent des données sensibles, au sens de de l’article 9§1 du RGPD.

Les Données Personnelles sont destinées au CHU d’Angers, à tout cocontractant autorisé par le CHU d’Angers et à toutes personnes désignées par le CHU d’Angers pour les besoins du déroulement d’un audit, ainsi qu’aux membres des autorités sanitaires concernées.

La durée de conservation des données est fixée par le CHU d’Angers, sur les conseils du titulaire, le cas échéant. Au terme de cette durée ou à la fin de la mission prévue au marché du titulaire, celui-ci s’oblige, au choix du CHU d’Angers :

* Soit à restituer l’ensemble des Données Personnelles traitées, de quelque façon que ce soit, sur le support électronique non réinscriptible défini par le CHU d’Angers (ci-après, le « Support »), dans un format interopérable ;
* Soit à anonymiser les Données Personnelles, selon un procédé irréversible (c’est-à-dire ne permettant pas la réidentification d’une Personne Concernée par un quelconque procédé d’individualisation, de corrélation ou d’inférence) validé par le CHU d’Angers, avant de les remettre au CHU d’Angers;
* Soit à détruire l’ensemble des Données Personnelles traitées, de quelque façon que ce soit.

Le titulaire s’interdit en tout état de cause de conserver tout ou partie des Données Personnelles ainsi que des données ayant été anonymisées (ci-après, les « *Données Anonymes* ») au terme de leur mission ou de la durée de conservation fixée par le CHU d’Angers.

Le CHU d’Angers peut, par exception, admettre la conservation temporaire de Données Personnelles ou de Données Anonymes du fait des caractéristiques techniques du système de sauvegarde du cocontractant ou de l’utilisateur externe (ex. : sauvegarde incrémentale). Le cas échéant, le titulaire s’oblige à :

* Assurer la confidentialité des Données Personnelles et/ou des Données Anonymes pendant toute la durée de conservation de la sauvegarde concernée ;
* Ne pas traiter, exploiter ou utiliser à quelques fins que ce soit, en dehors de la conservation de sauvegarde, les Données Personnelles et/ou les Données Anonymes ;
* Aviser le CHU d’Angers de toute violation de la confidentialité de la sauvegarde ;
* Informer le CHU d’Angers de la durée nécessaire à l’effacement de la sauvegarde concernée ;
* Notifier au CHU d’Angers l’effacement de la sauvegarde concernée.

Les caractéristiques techniques du traitement de Données Personnelles sont définies au marché.

Les Parties reconnaissent et acceptent que ces caractéristiques techniques sont susceptibles d’évoluer du fait de l’adoption de recommandations des autorités publiques compétentes en matière de protection des données à caractère personnel, et notamment de la Commission Nationale de l’Informatique et des Libertés (ci-après, la « *CNIL* »), de l’Agence des Systèmes d’Information Partagés en Santé (ci-après, l’ « *ASIP Santé* ») ou de l’Agence Nationale de Sécurité des Systèmes d’Information (ci-après, l’ « *ANSSI* »).

Le titulaire s’oblige à respecter l’ensemble des caractéristiques du Traitement concerné par le marché.

### Obligations des Parties concernant le Traitement de Données Personnelles

Les Parties s’obligent à respecter et faire respecter l’ensemble des obligations légales applicables en matière de protection de données à caractère personnel.

En sa qualité de sous-traitant, le titulaire s’oblige, envers le CHU d’Angers seul responsable des Données Personnelles, à :

* Traiter les Données Personnelles dans le cadre strict et nécessaire à l’exécution de la mission prévue au marché et exclusivement sur instructions écrites et préalables du CHU d’Angers, y compris en ce qui concerne les transferts de Données Personnelles vers un pays tiers ou à une organisation internationale ;
* Alerter le CHU d’Angers si une ou plusieurs instructions écrites constituent, directement ou indirectement, une violation du RGPD ou de toute réglementation communautaire ou nationale applicable au Traitement ;
* Notifier au CHU d’Angers tout transfert de Données Personnelles vers un pays tiers lorsque le titulaire est contraint d’y procéder en vertu du droit de l'Union ou du droit français, excepté lorsque la législation imposant le transfert interdit une telle information pour des motifs importants d’intérêt public ;
* Prendre les précautions, mesures et garanties nécessaires pour préserver la confidentialité et la sécurité des Données Personnelles et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés et plus généralement, mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données contre la destruction, la perte, l'altération, la diffusion ou l'accès autorisé, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute forme de traitement illicite ;
* Se conformer, en matière de sécurité et de confidentialité des systèmes et des Données Personnelles, aux normes techniques, aux bonnes pratiques applicables en matière de données à caractère personnel relatives à la santé ainsi qu’aux instructions émanant du CHU d’Angers ;
* Informer dans un délai maximal de vingt-quatre (24) heures ouvrées toute faille de sécurité détectée ou supposée ;
* Informer immédiatement par écrit le CHU d’Angers de toute modification, changement ou autre fait, notamment en matière de sécurité, le concernant et pouvant avoir un impact sur le traitement des Données Personnelles ;
* Prendre en compte toute mise à jour, correction, suppression ou autres modifications communiquées par le CHU d’Angers concernant les Données Personnelles ;
* Faire en sorte que les personnes en charge de l’exécution de la mission prévue au marché et ayant accès aux Données Personnelles soient soumises à une obligation écrite de confidentialité et de sécurité appropriée ;
* Faire respecter les obligations stipulées au présent article par son personnel ;
* Procéder à la destruction des Données Personnelles, à l’issue de la mission prévue au marché, quelle qu’en soit la cause, après les avoir restituées au CHU d’Angers, le cas échéant ;
* Ne conserver aucune copie des Données Personnelles à l’issue du marché, quelle qu’en soit la cause.

Le titulaire s’oblige à assister le CHU d’Angers dans la mise en œuvre du Traitement.

Ayant conscience de ce que certaines des Données Personnelles traitées par le CHU d’Angers sont particulièrement sensibles, le titulaire s’oblige à faire ses meilleurs efforts pour assister le CHU d’Angers dans :

* la réponse aux demandes d’accès, de rectification, d’opposition, et/ou de droit à l’oubli, à la limitation du Traitement, à la portabilité des Données Personnelles formulées par des Personnes Concernées ;
* la réponse à toute demande d’informations de la CNIL ou de toute autre autorité de protection des données compétentes ;
* la garantie du respect des obligations de sécurité des Données Personnelles, de notification de toute violation de Données Personnelles à la CNIL ou à toute autre autorité de protection des données compétente ainsi qu’aux Personnes Concernées, de réalisation d’une analyse d’impact et, le cas échéant, de consultation préalable de la CNIL ou de toute autre autorité de protection des données compétente.

Le CHU d’Angers est seul responsable de l’accomplissement des éventuelles formalités préalables adéquates auprès de la CNIL.

Le titulaire est en revanche tenus d’aviser le CHU d’Angers de la nécessité d’accomplir des formalités et du régime de formalité applicable, le cas échéant, et de fournir au CHU d’Angers l’aide et l’assistance – notamment en transmettant les informations techniques, juridiques et organisationnelles requises – nécessaire à ces formalités.

### Registres

Eu égard à la nature des Données Personnelles et au caractère habituel du Traitement, le titulaire s’oblige à tenir un registre écrit, sur support physique ou électronique, de toutes les catégories d’activités de traitement effectuées pour le compte du CHU d’Angers (ci-après, le « Registre »). Le Registre comporte les éléments d’information suivants :

* Noms et coordonnées :
  + du ou des sous-traitants approuvés par le CHU d’Angers ;
  + de chaque responsable de traitement pour le compte duquel le titulaire intervient ;
  + du représentant du responsable de traitement ou du sous-traitant approuvé ainsi que de leur délégué à la protection des données respectif, le cas échéant ;
* Catégories de traitements effectués pour le compte de chaque responsable de traitement pour le compte duquel le titulaire intervient ;
* Transferts de Données Personnelles vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, le cas échéant, les documents attestant de l'existence de garanties appropriées ;
* Description générale des mesures de sécurité techniques et organisationnelles par le titulaire, dans la mesure du possible.

Le Registre sera tenu par le titulaire à disposition du CHU d’Angers – à l’exception des mentions relatives à des traitements de données ne relevant pas de leur responsabilité – de la CNIL ou de toute autre autorité de protection des données compétentes.

Le CHU d’Angers déclarent tenir un registre écrit, sur support physique ou électronique, recensant tous les traitements de données à caractère personnel effectués, directement, indirectement ou par personne interposée sous leur responsabilité.

## Données de santé à caractère personnel – Agrément hébergement données de santé

Le titulaire garantit qu’il dispose au jour de la signature du contrat de l’ensemble des autorisations légales et administratives pour la sécurisation et l’hébergement de données de santé.

En particulier, il est agréé, au sens des dispositions de l'article L.1111-8 du Code de la santé publique, autorisée par les services compétents à réaliser des prestations d'hébergement de données de santé à caractère personnel.

En sa qualité d’hébergeur de données de santé à caractère personnel, il s’engage à mettre à disposition du CHU d’Angers les autorisations dont il dispose et les règles légales auxquelles il est soumis en tant qu’hébergeur, le CHU d’Angers pouvant les demander par simple demande écrite.

## Comité de suivi sécurité

Il sera institué un comité de suivi et de sécurité du projet permettant une communication efficace des informations nécessaires à la réussite des prestations effectuées par le titulaire.

Sont membres de plein droit du comité de suivi :

* le chef de projet du CHU d’Angers ;
* le responsable de la sécurité des SI du CHU d’Angers ;
* le chef de projet du titulaire ;
* le responsable de la qualité du titulaire ;
* le responsable de la sécurité des SI du titulaire ;
* toute personne jugée utile compte tenu de l'ordre du jour par l'une des parties.

Ce comité de suivi a notamment pour objet de discuter entre les parties des éléments suivants :

* conformité de l'hébergement ;
* performance dans l'accès au serveur ;
* sécurité physique de l'accès au serveur ;
* sécurité logique de l'accès au contenu du serveur ;
* réalisation et conservation des sauvegardes ;
* suivi des interruptions éventuelles de l'accès aux données de santé ;
* exécution générale du marché ;
* conformité des prestations ;
* respect de l’obligation de collaboration ;
* validations des améliorations pour accroître la sécurité ;
* questions techniques liées à la sécurité (collaboration dans la gestion des droits et la gestion des incidents, détection des anomalies et préconisation d’améliorations, exploitation des résultats des audits de contrôle des prestations sécurité, …) ;
* obligations liées à la loi du 6 janvier 1978 relative à l’Informatique, aux fichiers et aux libertés ;
* transfert des moyens de sécurité matériels et logiciels mis en place, en cas de réversibilité de l’opération.

## Qualité et niveaux de service

Le titulaire fournira des indicateurs de qualité de service et de performances visant notamment à vérifier l’adéquation entre les besoins de sécurité définis par le CHU d’Angers et le niveau de service proposé. Ces indicateurs de qualité de service porteront à minima sur :

* Taux de disponibilité du système (en heures ouvrées / non ouvrées) ;
* Le temps de détection d’incident garanti ;
* Le temps garanti d’intervention en cas d’incident (GTI) ;
* Le temps garanti de remise en état du service hébergé (GTR) ;
* La gestion des sauvegardes (fréquence, réussite ou échec des sauvegardes, rapport des tests de restauration) ;
* La performance du service (le temps de réponse d’une application ou de certaines requêtes, la durée maximale de certains traitements, la vitesse de transfert des données, …) ;
* La mise en œuvre de processus de traçabilité ;
* Le nombre d'incidents ;
* Le respect de la politique de sécurité (procédures de contrôles, reporting, mesures de sécurité…) ;
* Les délais de correction des anomalies ;
* L’intégrité des données.

Le CHU d’Angers devra pouvoir accéder à tout moment aux données brutes qui servent pour le calcul des indicateurs.

## Audits de sécurité et contrôles

Le titulaire accepte que le CHU d’Angers puisse vérifier les conditions d'hébergement des données confiées et du service pour contrôler que les exigences de sécurité sont satisfaites par les dispositions prises, et pour ce faire, que le CHU d’Angers puisse pénétrer dans les lieux du service.

Le titulaire s'engage à ne pas bloquer l'intervention de l'auditeur et à mettre à sa disposition l'ensemble des informations permettant à ce dernier de prendre la mesure des conditions d'hébergement des données et du service.

Les audits pourront être réalisés par le CHU d’Angers, ou délégués à un tiers.

Le droit d'accès de l'auditeur a pour objet de vérifier les conditions d'hébergement des données et du service confiés par le CHU d’Angers au regard des obligations du présent marché. En conséquence, l'auditeur pourra notamment contrôler :

* les configurations d'hébergement et d'exploitation des données recueillies ou produites par le CHU d’Angers ;
* les utilisateurs ayant accès aux données ;
* les procédures de mise à jour des données et de sécurité ;
* les procédures techniques et organisationnelles de sécurité.

Dans le cas où l’audit nécessite la réalisation de tests d’intrusions, ceux-ci seront encadrés par un protocole commun et une notification de tests d’intrusion entre le titulaire, l’exécutant de l’audit et le CHU d’Angers.

L’auditeur sera soumis à la plus stricte confidentialité et au secret professionnel.

## Application des plans gouvernementaux

Dans le cadre de l’application de plans gouvernementaux, le Premier Ministre peut décider la mise en œuvre d’un ensemble de mesures spécifiques destinées à lutter contre des attaques notamment terroristes visant les systèmes d’information de l'État ou les systèmes d’information et réseaux de télécommunications des opérateurs d’infrastructures vitales.

Dans le cadre de ce marché, le titulaire pourrait être concerné par ces alertes décidées au niveau gouvernemental, et s’engage à appliquer les consignes de sécurité données par le donneur d’ordres. Ces mesures sont susceptibles d’évoluer. Les modifications seront régulièrement transmises durant l’exécution du marché.

## Sécurité dans les développements applicatifs

Le titulaire est tenu d’assurer la sécurité des développements conformément à l’état de l’art dans chacune des technologies mises en œuvre.

Les règles applicables à la sécurité dans les développements peuvent-être :

(liste non exhaustive)

* environnement applicatif maintenu en tenant compte des recommandations d'application de correctifs par les éditeurs ;
* contrôle rigoureux des entrées utilisateurs ;
* sécurisation des accès aux fonctions d’administration ;
* installation du minimum de fonctions nécessaires lors de l’installation ;
* principe du moindre privilège ;
* utilisation de mots de passe dans le code interdite ;
* mise en œuvre d’une gestion efficace des erreurs.

Le titulaire s’engage à permettre au CHU d’Angers la réalisation d’une revue de code lui permettant de s’assurer d’une implémentation conforme aux exigences de sécurité.

Les audits de vulnérabilité pourront être réalisées par le CHU d’Angers, ou déléguées à un tiers.

La correction d’éventuelles anomalies détectées lors de la revue de code sont à la charge du titulaire.

## Gestion des évolutions

Les évolutions fonctionnelles ou techniques ne doivent pas remettre en cause le respect des exigences de sécurité ou compromettre une éventuelle opération de réversibilité.

En cas d’évolution, le prestataire devra vérifier que sa mise en œuvre est conforme aux exigences du présent marché et en apporter la justification auprès du CHU d’Angers, avant validation par ce dernier.

## Réversibilité

Le prestataire s’engage à apporter l’assistance nécessaire durant la période de migration pour faciliter le transfert des moyens de sécurité matériels et logiciels, et la reprise de leur exploitation par le CHU d’Angers, ou par un autre prestataire de service.

Le prestataire s’engage à garantir, lors du transfert, la sécurité des données et des applications qui lui ont été confiées, conformément à ses obligations.

En outre, la phase de réversibilité ne doit pas, en principe, modifier la qualité, les termes et les conditions des services fournis.

En cas d'arrêt des prestations confiées au titulaire par le CHU d’Angers, l'ensemble des matériels, logiciels et documentations confiés au titulaire doivent être restitués.

Le déménagement de cet ensemble des locaux du titulaire sera assuré aux frais du titulaire dans un délai maximum d'un mois après l'arrêt des prestations confiées au titulaire.

Une non restitution de tout ou partie de cet ensemble sera considérée et traitée comme une perte.

Une restitution partielle peut être demandée par le CHU d’Angers, en cas d’arrêt d’une partie des prestations avant la fin du marché. Dans ce cas, le titulaire en sera informé au moins un mois avant la fin des prestations.

À la fin de l’exécution du marché, le titulaire est tenu :

* de transférer à l’équipe du futur titulaire les informations sur le contexte fonctionnel et technique de l’ensemble applicatif ainsi que sur les aspects de suivi du projet ;
* de préparer un support informatique défini par le CHU d’Angers contenant tous les éléments (documentations, programmes, chaînes de compilation…) gérés par le titulaire actuel et qui seront, à l’issue de cette prestation, placés sous la responsabilité du futur titulaire (cette mise à disposition devra être faite sous un format pouvant permettre au futur titulaire d’installer, le cas échéant, l’ensemble de ces éléments sur une plate-forme de son choix pour examen approfondi par celui-ci) ;
* d’assurer une formation fonctionnelle approfondie (du type formation utilisateur et administrateur) aux personnels du futur titulaire, avec travaux pratiques sur poste de travail, en présence de représentants du donneur d’ordres. Cette formation devra s’appuyer sur les documentations utilisateurs et techniques rédigées par le titulaire.

En particulier, au titre de cette prestation, le titulaire :

* lance la prestation avec le futur titulaire et les représentants du donneur d’ordres. Il s’agit, au plus, de deux jours de réunion en vue de valider le planning et les modalités pratiques de cette phase ;
* met à disposition tous les éléments et documents produits par ou remis au présent titulaire ;
* présente l’ensemble des composants techniques ou fonctionnels du projet ;
* répond aux questions du futur titulaire concernant l’organisation pratique des configurations et des documents techniques sous 48 heures ;
* présente l’organisation de la maintenance corrective actuelle et l’environnement de développement et d’exploitation (répertoires, installation, procédures mises en œuvre, périodicité et ordonnancement des opérations d’exploitation, etc.) ;
* accueille, durant deux semaines, deux ou trois personnes du futur titulaire afin de leur permettre d’observer l’activité assurée par l’équipe projet en place (assistance téléphonique, exploitation de serveurs de développement, etc.) ;
* communique au futur titulaire les réponses apportées aux demandes d’assistance téléphonique traitées.

## Restitution des données

En cas de réversibilité, le titulaire s’engage à restituer les données sans en garder de copie dans un délai défini avec le CHU d’Angers.

Les modalités de restitution seront précisées.

Le prestataire doit maintenir l’accès aux données tant que les données n’ont pas été réceptionnées par le CHU d’Angers ou que le service du nouveau titulaire n’est pas accessible.

# Exigences de sécurité

## Prévention d’une attaque ou d’un incident

Le titulaire doit mettre en œuvre des mesures techniques et organisationnelles permettant de gérer des incidents ou des attaques. Ces mesures doivent garantir que le CHU d’Angers soit immédiatement informé d’un incident ou d’une attaque et lui permettre de suivre leur évolution.

Le titulaire décrira également les procédures dégradées qui peuvent être mises en œuvre en fonction des scénarios de sinistre rencontrés.

Il est également souhaité dans le cadre de ce projet d’être informé en cas d’incident des commandes qui ont été traitées ou non de manière à pouvoir déclencher un mode dégradé.

## signalement des incidents graves de sécurité

Le décret d’application N°2016-1214 du 12 septembre 2017 précise que les incidents graves de sécurité des systèmes d’information du secteur santé devront être signalés sans délai à partir du 1er octobre 2017.

En cas d’incident ou d’attaque, le titulaire devra mettre à disposition du CHU d’Angers tous les éléments permettant à ce dernier de faire sa déclaration d’incident sur le portail de signalement des évènements sanitaires indésirables : https://signalement.social-sante.gouv.fr

## Sauvegardes

Les sauvegardes doivent être réalisées en double exemplaire dans des locaux distincts. La fréquence des sauvegardes doit être définie par le CHU d’Angers.

Des tests réguliers des sauvegardes doivent être réalisés.

Le CHU d’Angers doit être informé du bon déroulement des sauvegardes et des résultats des tests et doit pouvoir à tout moment modifier la fréquence des sauvegardes.

La confidentialité des données relatives aux sauvegardes doit être garantie.

## Isolement et confinement

Le titulaire doit garantir que le service et les données du CHU d’Angers sont isolés de ses autres activités.

## Imputabilité, traçabilité

Le titulaire tiendra à la disposition du CHU d’Angers les traces concernant :

* l’entrée en session d'un utilisateur : date, heure, identifiant de l'utilisateur et du terminal ; réussite ou échec de la tentative ;
* les actions qui tentent d'exercer des droits d'accès à un objet soumis à l'administration des droits (ex : visualisation de données soumises à habilitations) : date, heure, identité de l'utilisateur, nom de l'objet, type de la tentative d'accès, réussite ou échec de la tentative ;
* la création/suppression d'un objet soumis à l'administration des droits : date, heure, identifiant de l'utilisateur, nom de l'objet, type de l'action ;
* les actions d'utilisateurs autorisés affectant la sécurité de la cible : date, heure, identité de l'utilisateur, type de l'action, nom de l'objet sur lequel porte l'action.
* les accès et les évènements systèmes de tous les équipements dont il a la charge.

Le titulaire s’engage à garantir la sécurité des traces autant sur le plan de la disponibilité, que de l’intégrité ou de la confidentialité.

Le titulaire doit garantir que toutes les informations présentes dans les journaux sont exploitables au regard de l’état de l’art.

## Plan de secours

Le titulaire s’engage à mettre en œuvre et à maintenir un plan de secours informatique.

Ce plan de secours comprend :

* Une description des services
* Les temps de reprise validés par le CHU d’Angers
* Les responsabilités respectives
* Les scénarios de reprises
* Les tests du plan de secours

A ce titre, le titulaire dispose d’une infrastructure de secours permettant de basculer l’activité.

En cas de déclenchement du plan de secours, le titulaire doit informer le CHU d’Angers.

## Confidentialité et intégrité des flux

Le titulaire est tenu d’assurer la confidentialité et l’intégrité des flux.

Le choix et le dimensionnement des algorithmes cryptographiques doivent être conformes aux règles et recommandations du Référentiel Général de Sécurité (RGS).

## Gestion des flux

Le service proposé devra respecter les règles d’usages du réseau informatique du CHU d’Angers. Aucun flux non justifié ne sera autorisé. A ce titre, le prestataire communiquera une matrice des flux qui précisera obligatoirement les éléments suivants : nature de l’information, finalité de l’échange, adresse source, port source, adresse cible, port cible, protocole de communication et volumétrie.

Les flux générés par le progiciel ne devront jamais perturber les échanges entre les autres applications en occupant inutilement la bande passante.

Les variantes sécurisées des protocoles de communication seront utilisées. Les communications doivent en effet être chiffrées et ce surtout pour les communications sur Internet. Le titulaire décrira donc l’ensemble des mécanismes et mesures mis en œuvre pour garantir la confidentialité et l’intégrité des flux (flux d’administration, flux contenant des informations sensibles, flux circulant sur un réseau public, …).

## Authentification

L’accès aux services et aux données est réservé au CHU d’Angers et sont obligatoirement nominatifs.

Si l’authentification se fait par identifiant/mot de passe :

* l’utilisation sur la durée de mot de passe par défaut est strictement interdite
* une politique de gestion des mots de passe est obligatoire

L’utilisation de protocoles dont l’authentification est en clair est interdite.

## Sécurité des postes de travail

L’application devra impérativement se faire sans remise en cause de la politique de protection contre les codes malveillants.

Les postes de travail du CHU d’Angers sont régulièrement mis à jour vis-à-vis des correctifs de sécurité (navigateur Internet y compris). Le service devra garantir la compatibilité avec les correctifs de sécurité des systèmes d’exploitation Microsoft et des navigateurs de type Internet Explorer et Firefox.

De manière générale, le service devra garantir la non altération de la configuration des postes de travail du CHU d’ Angers et l’indépendance du service vis-à-vis de la configuration de ces postes. Ainsi, quel que soit les évolutions logiciels des postes de travail, le service sera toujours compatible.

## Sécurité du site Internet accédé par le CHU d’Angers

Le titulaire garantira la sécurité du site Internet accédé par le CHU d’Angers contre les attaques classiques (compromission de site, injection de code malveillant depuis le site, accès aux données, …). A ce titre, il décrira les mesures de sécurité mises en œuvre pour garantir cette sécurité et la sécurité du SI du CHU d’Angers vis-à-vis de ces attaques (sécurité des développements, protection des infrastructures et serveurs contre les codes malveillants, correctifs de sécurité…).

## Gestion de la déconnexion

L’utilisateur doit pouvoir se déconnecter du logiciel à tout moment. Aucun autre utilisateur ne peut utiliser sa session s’il l’a fermée. En aucun cas la déconnexion de l’utilisateur n’entraîne l’apparition d’une fenêtre permettant à un autre utilisateur de se connecter sur la session du précédent utilisateur.

## Maintenance évolutive et information

Le titulaire assure la maintenance évolutive de l’hébergement des infrastructures informatiques.

Il doit informer le CHU d’Angers de toute modification dans l'organisation générale du réseau et de toutes avancées techniques ou technologiques susceptibles d'avoir des conséquences directes sur la prestation d'hébergement.

La maintenance évolutive et les modifications ou évolutions techniques ne doivent en aucun cas diminuer les niveaux de service.

Les évolutions fonctionnelles ou techniques ne doivent jamais remettre en cause le respect des exigences de sécurité ou compromettre une éventuelle opération de réversibilité. En cas d’évolution, le prestataire devra vérifier que sa mise en œuvre est conforme aux exigences contractuelles et en apporter la justification auprès du CHU d’Angers, avant validation par ces derniers.

## Suivi des contrats de maintenance tiers

Le titulaire doit sécuriser les interventions des sociétés de maintenance. Il doit notamment mettre en place des mesures permettant d’empêcher l’extraction d’information ou la récupération de supports de données.

## Charte fournisseur

Le titulaire et tous les intervenants devront respecter la « Charte d'accès au SI du CHU d’Angers». Le titulaire s’engage à respecter la confidentialité des documents et des informations en rapport avec le CHU d’Angers.