Table des matières

[1 Préambule 2](#_Toc512001359)

[2 Exigences générales de sécurité SI 2](#_Toc512001360)

[2.1 Démarche utilisée 2](#_Toc512001361)

[2.2 Plan d’Assurance Sécurité SI 2](#_Toc512001362)

[2.3 Organisation de la sécurité SI pour la prestation 3](#_Toc512001363)

[2.3.1 Désignation d’un RSSI pour la prestation 3](#_Toc512001364)

[2.3.2 Organisation sécurité SI mise en place par le titulaire 3](#_Toc512001365)

[2.4 Gestion des intervenants du titulaire 4](#_Toc512001366)

[2.4.1 Habilitation du personnel 4](#_Toc512001367)

[2.4.2 Conditions d’accès aux sites du chu d’angers 5](#_Toc512001368)

[2.4.3 Information – Sensibilisation 5](#_Toc512001369)

[2.5 Gestion des accès aux informations 6](#_Toc512001370)

[2.6 Gestion des ressources et biens liés à la prestation 6](#_Toc512001371)

[2.6.1 Inventaire des ressources 6](#_Toc512001372)

[2.6.2 Cas particuliers des systèmes portables et du travail à distance (e.g. astreinte) 7](#_Toc512001373)

[2.7 Gestion des risques de sécurité SI 7](#_Toc512001374)

[3 Exigences spécifiques de sécurité SI pour les prestations hors site du chu d’angers 8](#_Toc512001375)

[3.1 Raccordement au SI du chu d’angers 8](#_Toc512001376)

[3.2 Sécurité et accès physiques des locaux du titulaire 8](#_Toc512001377)

[4 Réversibilité 8](#_Toc512001378)

[5 Conformité 9](#_Toc512001379)

# Préambule

La fourniture d'un Plan d’Assurance Sécurité (PAS) est demandée dans l'appel d'offres. Rédigé par le titulaire, il décrit l'ensemble des dispositions spécifiques que celui-ci prendra pour garantir le respect des exigences de sécurité du donneur d'ordre.

Le PAS est un document contractuel : il constitue la réponse du futur titulaire aux exigences de sécurité définies dans le cahier des charges.

L'exigence de fourniture d'un PAS se substitue à la clause générique de sécurité du titulaire.

Le PAS est un cadre de réponse : il offre une structure pour la réponse des soumissionnaires aux exigences de sécurité, ce qui permet de mieux évaluer la pertinence de la couverture des exigences. Il facilite ainsi la comparaison des différentes offres au regard des garanties proposées.

Grâce à une clause spécifique, le PAS peut être modifié lors de l'exécution du marché pour répondre à des évolutions du système, de son environnement ou du périmètre de l'opération. Cette souplesse garantit que les mesures prises par le titulaire seront toujours adaptées aux exigences de sécurité.

# Exigences générales de sécurité SI

## Démarche utilisée

L’ensemble des exigences indiquées ci-après sont applicables indépendamment de la localisation des intervenants du titulaire, qu’ils soient basés sur site du CHU d’Angers ou dans les locaux du titulaire.

Les éventuels intervenants du ou des sous-contractant(s) du titulaire sont soumis aux mêmes contraintes. Ceux-ci sont inclus dans la dénomination « intervenants du titulaire » ci-après.

## Plan d’Assurance Sécurité SI

Le Plan d’Assurance Sécurité Système d’Information (PAS) comprend et détaille l’ensemble des éléments permettant de piloter et de maîtriser la sécurité SI de l’environnement relatif aux prestations, et les services/ processus qui y contribuent, qu’ils soient purement internes au titulaire ou qu’ils comportent des interactions avec le CHU d’Angers.

Le Plan d’Assurance Sécurité, document contractuel pour la durée de la prestation, constituera un référentiel en termes d’audit sur le management de la sécurité dans le cadre de la prestation assurée par le titulaire.

Le titulaire prépare le PAS au cours de la première phase de mise en place, avec la participation du CHU d’Angers pour ce qui le concerne.

Le PAS est soumis pour approbation :

* Au Responsable de la sécurité des systèmes d’information du CHU d’Angers ou son représentant,
* Au Comité de Pilotage.

Il doit être approuvé avant le démarrage de la phase opérationnelle.

Le titulaire a l’initiative des évolutions du PAS. Il doit le faire évoluer en fonction des besoins. Il doit au minimum procéder à une révision annuelle et réaliser la mise à jour si nécessaire.

Le Plan d’Assurance Sécurité comprend l’ensemble des processus et procédures mentionnées ci-après dans ce chapitre.

Ce document recense l’ensemble des conditions d’exécution des prestations qui précisent les dispositions du contrat, telles qu’exposées ci-après et notamment :

* Exigences générales de sécurité
  + Organisation de la sécurité SI pour la prestation,
  + Gestion des intervenants du titulaire,
  + Gestion des ressources et biens liés à la prestation,
  + Gestion des risques de sécurité SI,
* Exigences spécifiques de sécurité pour les prestations hors site du CHU d’Angers
  + Raccordement au SI du CHU d’Angers
  + Sécurité et accès physiques des locaux du titulaire,
  + Gestion des incidents de sécurité sur le SI du titulaire,
  + Gestion de la continuité d’activité du SI du titulaire.

## Organisation de la sécurité SI pour la prestation

### Désignation d’un RSSI pour la prestation

Le CHU d’Angers demande à ce que soit désigné un Responsable de la Sécurité SI (RSSI) dans le cadre de la prestation. Ce RSSI sera l’interlocuteur privilégié du RSSI du CHU d’Angers pour tout point sensible touchant à la sécurité SI, par exemple en cas d’incident sécurité SI.

### Organisation sécurité SI mise en place par le titulaire

Le titulaire décrit l’organisation de la sécurité SI qu’il met en place dans le cadre de la prestation, avec des responsabilités clairement identifiées et attribuées ; cette organisation doit prendre en compte :

* Le partage des responsabilités au sein de ses équipes et le processus de maintien du Plan d’Assurance Sécurité,
* Le suivi des risques majeurs sur les ressources,
* Le suivi des incidents liés à la Sécurité des Systèmes d’Information (SSI) dont il a la charge,
* La mise en œuvre des contrôles en interne,
* Le processus d’approbation pour la gestion des ressources informatiques internes au titulaire (ressources nécessaires à l’exécution de la prestation),
* La communication sur le thème de la SSI à l’égard de ses personnels et éventuels sous-traitants,
* La gestion des relations avec les autorités de l’Etat ou réglementaires, si nécessaire (exemple des réquisitions judiciaires) sous l’autorité du RSSI du CHU d’Angers,
* La mise en place des traces de toutes actions exécutées par le titulaire,
* L’identification et la prise en compte des risques dans le cas d’accès au SI dédié à la prestation par une tierce partie (e.g. administrateur des ressources du titulaire nécessaires à l’exécution de la prestation, mainteneur de ces ressources), et les contrôles spécifiques associés,

La contractualisation des exigences de SSI cohérentes avec celles du CHU d’Angers quant à la protection de son SI et de ses informations dans le cas d’accès au SI par une tierce partie.

Ces exigences doivent être reconduites sur les sous-contractants, le CHU d’Angers étant informé de cette sous-traitance à l’avance. Ces sous-contractants sont soit directement impliqués sur la prestation du CHU d’Angers, soit interviennent dans les locaux dédiés à cette prestation (e.g. maintenance d’application, réseau ou bureautique : maintenance matérielle des postes de travail, ...).

## Gestion des intervenants du titulaire

Lorsque le personnel du titulaire travaille sur le SI du CHU d’Angers, il est dédié sur ces activités. Pour l’ensemble du périmètre, il doit être nommément identifié et avoir été habilité par le CHU d’Angers. Le titulaire s’engage à ne faire intervenir sur le SI du CHU d’Angers que des personnels habilités et identifiés.

Aucun accès, ni physique, ni logique, au CHU d’Angers ne pourra être accordé sans avis favorable de ce dernier.

### Habilitation du personnel

En raison des droits d’accès au SI du CHU d’Angers ainsi que des droits d’accès physiques à certains sites sensibles qui seront confiés aux intervenants dans le cadre de leur mission, le titulaire doit impérativement transmettre au CHU d’Angers, au moins 2 semaines avant leur intervention, l’identité de ses intervenants en fournissant carte d’identité et CV. Cette exigence s’applique également en cas de changement d’intervenant au cours de la mission.

Le personnel doit s’engager à respecter la charte d’utilisation des ressources informatiques et des télécommunications du CHU d’Angers.

L’objet de cette charte est de préciser l’ensemble des règles générales que le personnel du titulaire doit respecter dans l’utilisation des outils informatiques du CHU d’Angers, de façon à éviter de mettre en péril le bon fonctionnement du système ou sa sécurité.

Si ce document évolue, le RSSI du CHU d’Angers transmettra au titulaire les versions actualisées de ces documents. Le titulaire a obligation d’utiliser la dernière version fournie.

Le titulaire communique au RSSI du CHU d’Angers un exemplaire de cette charte signée.

Les chargés de missions d’audit ou de contrôle mandatés par le CHU d’Angers doivent pouvoir avoir accès à ces documents.

Il est rappelé que conformément aux clauses contractuelles le titulaire et l’ensemble de son personnel sont tenus par un engagement de confidentialité.

Le non-respect des règles de confidentialité applicable à tout utilisateur du SI du CHU d’Angers pourra être considéré comme une faute grave.

### Conditions d’accès aux sites du chu d’angers

Il appartient au titulaire de prendre connaissance et d’appliquer les procédures et règlements propres à chaque site où il est susceptible d’intervenir. Parmi les contraintes propres à chaque site, on peut noter :

* Les horaires d’ouverture,
* Les éventuels contrôles individuels d’accès,
* Les conditions de livraison et de réception de matériel.

Suite à la procédure d’habilitation, le service numérique du CHU d’Angers fournira aux collaborateurs du titulaire devant intervenir sur des sites de l’établissement des accès permanents. Si la mission de l’intervenant le justifie, l’accès peut être 24h/24 7j/7.

Pour l’aspect sécurité, au niveau des départs, le titulaire informe le chef de projet du CHU d’Angers 10 jours ouvrés avant le départ effectif de la personne, afin que le service numérique de l’établissement puisse clore les accès et habilitations correspondants. Ce délai est le délai minimum spécifique à la sécurité. Il ne remet pas en cause les délais de prévenance nécessaires au bon fonctionnement de la prestation.

Le titulaire est responsable de récupérer l’ensemble des moyens physiques d’accès au SI du CHU d’Angers qui ont été fournis à son personnel dans le cadre de la prestation pour l’établissement (e.g. carte CPx, badge d’accès à un site) et de les restituer au service numérique du CHU d’Angers. Tout moyen matériel non restitué sera facturé au titulaire.

Le titulaire décrit ces procédures dans le PAS.

### Information – Sensibilisation

Les acteurs concernés doivent être informés / sensibilisés sur les points suivants a minima les exigences du CHU d’Angers en matière de sécurité SI et les procédures associées.

Dans ce cadre, le titulaire accompagnera l’arrivée d’un entrant dans la prestation par l’explication et la remise d’un livret d’accueil rappelant ces éléments ; il s’assurera également du maintien à niveau de la sensibilisation et de la connaissance des règles sécurité SI répondant aux exigences du CHU d’Angers en la matière.

## Gestion des accès aux informations

Pour chaque personnel concerné, un préalable à l’attribution de droits d’accès au SI du CHU d’Angers, est son habilitation par le service numérique de l’établissement. Le personnel du titulaire peut ou doit disposer des droits de niveau Administrateur sur les serveurs / équipements qu’il exploite. Il est soumis pour cela aux règles de sécurité du CHU d’Angers.

Par exemple la gestion des privilèges (au sens droits système ou droits applicatifs étendus) doit être strictement contrôlée, avec des privilèges associés à chaque produit système, tels que système d’exploitation, gestion de base de données, application par application, et en fonction des missions de chacun.

Les intervenants du titulaire doivent utiliser des comptes nominatifs, et les outils (e.g. carte à puce, token, identifiants …) qui leur ont été fournis à ce titre, pour accéder au SI de l’établissement : tout authentifiant utilisateur est personnel et incessible. Chaque intervenant du titulaire est responsable des actions réalisées avec son «identifiant/authentifiant». De même, les « identifiants » génériques sont strictement interdits sauf dérogation formalisée et accordée par le RSSI avec justification explicite.

En particulier, il doit y avoir :

* Une révocation immédiate des droits lors d’un changement d’affectation ou d’entreprise,
* Des droits d’accès des utilisateurs revus et contrôlés à intervalle régulier, suivant une procédure formalisée.

La gestion des mots de passe des personnels doit respecter la politique en vigueur de l’établissement.

Le titulaire doit décrire comment il assure ces services pour la sécurité des informations.

La non-information du RSSI du CHU d’Angers en cas d’incident de sécurité sera considérée comme une faute grave.

## Gestion des ressources et biens liés à la prestation

### Inventaire des ressources

Le titulaire réalisera l’inventaire et le marquage des ressources nécessaires dans le cadre de la réalisation de la prestation et maintiendra à jour cet inventaire.

Cet inventaire inclut les ressources du CHU d’Angers et du titulaire. Le PAS décrira le processus de fourniture de cet inventaire.

Les ressources à identifier peuvent être par exemple :

* Des informations ou données (traitement, stockage, sauvegarde, archivage) :
* bases de données, fichiers, documents, manuels utilisateurs, documents de formation, procédures d’exploitation ou de maintenance, plans de continuité, archives,
* Des logiciels : applications, systèmes d’exploitation, outils de développement, outils de traçage des actions exécutées,
* Des matériels : stations de travail, PC ou ordinateurs portables, équipements de simulation, équipements de communications (e.g. routeurs, switchs), supports magnétiques,
* Des composants d’environnement : climatisation, protection incendie, câblage, ...
* Des services : services de traitement d’information ou de communications.

Le service numérique du CHU d’Angers peut en exiger la fourniture à tout moment du contrat.

Le PAS doit décrire le niveau et les mesures de protection mises en place pour toutes les phases : copie, stockage, transmission (e.g. courrier, fax, courrier électronique), archivage, destruction.

Sont concernés l’ensemble des supports pouvant contenir de l’information sensible ou nécessaire à un système sensible : disques durs, disques optiques, clés USB, rapports papier, enregistrements vocaux, listings, données de test, documentation système, ...

Ces supports doivent être identifiés et listés puis marqués, manipulés, stockés et détruits de manière sûre, avec une gestion des accès à ces supports.

Le titulaire assure le maintien à niveau de ses ressources, par exemple en ce qui concerne les patchs de sécurité, et les dispositifs d’anti-virus.

### Cas particuliers des systèmes portables et du travail à distance (e.g. astreinte)

La protection et l’usage des systèmes portables (e.g. PC portables, PDA, tablettes, smart phones,) doivent faire l’objet d’une politique formalisée, qui tient compte des exigences en protection physique, contrôle d’accès, sauvegardes et anti-virus. Elle décrit aussi les règles en cas de connexion à un réseau ou d’utilisation dans les lieux publics.

Elle est décrite dans le Plan d’Assurance Sécurité, et donc soumise à l’approbation du RSSI du CHU d’Angers.

Cette politique impose en particulier que le travail à distance ne peut être effectué que sur du matériel respectant les normes sécurité du CHU d’Angers. L’usage de tout poste de travail de type personnel, familial, public est interdit.

## Gestion des risques de sécurité SI

Le titulaire réalise périodiquement une analyse des risques en ce qui concerne le périmètre de sa prestation par rapport aux exigences de sécurité SI. Il s’assure en particulier par cette démarche que les mesures de protection mises en place sont toujours cohérentes avec les exigences contractuelles du CHU d’Angers et met en place les actions correctrices nécessaires à ce sujet.

A ces fins, le titulaire met en place des contrôles et des audits en interne, afin de :

* S’assurer du respect des règles et procédures de sécurité SI,
* Identifier en cas de non-respect les causes,
* Proposer, dans le cadre du plan d’amélioration continu, des recommandations au service numérique du CHU d’Angers en termes d’évolutions du PAS ou des référentiels ad hoc,
* Formaliser des demandes de dérogations à durée définie si nécessaire,
* Mettre en place sur son périmètre les actions correctrices en retour de ces contrôles et des non-conformités constatées.

Le suivi des risques identifiés fera l’objet d’un paragraphe du Plan d’Assurance Sécurité et sera revu périodiquement en Comité de Pilotage.

# Exigences spécifiques de sécurité SI pour les prestations hors site du chu d’angers

Les éléments ci-dessous s’appliquent à tous les sites du titulaire à partir desquels la prestation s’effectue.

Pour parer aux urgences, un numéro privilégié (ligne rouge) sera prévu par le titulaire pour chacun des sites.

Il permet aux correspondants du CHU d’Angers d’être directement en relation avec le responsable local du titulaire.

## Raccordement au SI du chu d’angers

Si le titulaire réalise les prestations dans ses propres locaux, ceux-ci doivent être raccordés au SI du CHU d’Angers.

Le lien utilisé (e.g. Liaison Spécialisée, VPN) doit être sécurisé.

Les lieux de réalisation de la prestation et le niveau de sécurisation du raccordement au SI du CHU d’Angers doivent être validés par le service numérique du CHU d’Angers préalablement à leur mise en place.

Les travaux de mise en place sont réalisés par le titulaire en collaboration avec le CHU d’Angers.

Les coûts de mise en place et de fonctionnement des liens de raccordement sont à la charge exclusive du titulaire.

## Sécurité et accès physiques des locaux du titulaire

Ce périmètre physique (site, bâtiments, locaux, bureaux, plates-formes, matériels de servitude, locaux de télécommunications, locaux archivage, ...) doit être clairement identifié et protégé de manière adéquate par rapport à la sensibilité des systèmes qui y sont traités conformément aux exigences sécurité fournies par le CHU d’Angers.

Il doit exister un contrôle d’accès du site et des différentes zones identifiées comme liées à la prestation, en fonction des restrictions définies pour les personnes habilitées.

Une trace (journal d’audit) de ces contrôles doit être mise en œuvre et conservée de manière sécurisée et pouvoir être mis à disposition du service numérique de l’établissement ; le délai de conservation de ces traces devra être précisé.

Une procédure décrit les activités se situant dans ces zones sécurisées, les conditions d’accès et les personnes autorisées (y compris en ce qui concerne les sous-traitants, les intérimaires, les personnels de maintenance ou d’exploitation informatique, les personnels pour la logistique de site, etc.), les équipements autorisés (e.g. interdiction de tout matériel d’enregistrement sonore, vidéo ou autre).

Le titulaire doit pouvoir accueillir ponctuellement des intervenants du CHU d’Angers dans ses locaux, par exemple pour le contrôle de la prestation ou la gestion éventuelle des situations de crises.

# Réversibilité

* les modalités de reprise en interne par l'entreprise de la fonction externalisée,
* les modalités de transfert de ladite fonction à un autre titulaire,
* les conditions de transfert des droits et des matériels, les questions de la propriété intellectuelle des améliorations, etc.
* le coût de la réversibilité au moment de la conclusion du contrat et son évaluation périodique au cours de l'exécution dudit contrat.

# Conformité

Le titulaire indique dans le PAS comment il assure la conformité avec les thématiques suivantes :

•Les droits liés à la propriété intellectuelle,

•La protection des informations à caractère personnel (le CHU d’Angers a une commission spécifique traitant toutes les questions concernant la protection des informations à caractère personnel qu’il convient de solliciter).