Plan d’Assurance Sécurité - Modèle

*Objectifs :*

*Décrire un ensemble d’actions qui exécutées de la manière décrite et dans l’ordre décrit, aboutissent au résultat attendu.*

*Remarque :*

*Une procédure contient à minima*

*Le « quoi » faire*

*Le « quand »?*

*Et le « qui »?*

*Une procédure peut contenir le « comment » qui peut aussi faire l’objet d’un document séparé de type mode opératoire*

Table des matières

[1 Contexte 4](#_Toc505877074)

[2 Objet du document 4](#_Toc505877075)

[3 Document de référence 4](#_Toc505877076)

[4 Description du système 5](#_Toc505877077)

[5 Rappel des exigences générales de sécurité 5](#_Toc505877078)

[6 Rappel des exigences spécifiques de sécurité 5](#_Toc505877079)

[7 Organisation 5](#_Toc505877080)

[8 Organisation de <le titulaire> 6](#_Toc505877081)

[9 Organisation des HCL 6](#_Toc505877082)

[10 Responsabilités liées au Plan d’Assurance Sécurité 7](#_Toc505877083)

[11 Procédure d’évolution 7](#_Toc505877084)

[12 Applicabilité 7](#_Toc505877085)

[13 Mesures de sécurité 8](#_Toc505877086)

[13.1 Ressources humaines 8](#_Toc505877087)

[13.2 Transfert 8](#_Toc505877088)

[13.3 Installation, exploitation 8](#_Toc505877089)

[13.4 Réversibilité 8](#_Toc505877090)

[14 Matrice de couverture des exigences spécifiques 8](#_Toc505877091)

[15 Documentation de suivi 9](#_Toc505877092)

[16 Glossaire 9](#_Toc505877093)

[Annexe 1 : Classification en sécurité 10](#_Toc505877094)

# Contexte

Le Plan d'Assurance Sécurité (PAS) doit être demandé dans l'appel d'offres.

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

C'est aussi un cadre de réponse : il offre une structure pour la réponse des candidats aux exigences de sécurité, ce qui permet de mieux évaluer la pertinence de la couverture des exigences. Il facilite ainsi la comparaison entre les différentes offres.

Une fois le prestataire retenu, le PAS est annexé au contrat. Il se substitue aux éventuelles clauses génériques de sécurité du prestataire.

Le plan-type proposé ci-après pourra être joint à l'appel d'offres comme base de rédaction du Plan d’Assurance Sécurité qui sera fourni par les candidats en réponse à la consultation.

Les paragraphes en italique constituent des propositions de contenu du Plan d’Assurance Sécurité à fournir par le candidat. Ils devront être adaptés selon la nature du marché.

# Objet du document

Ce document décrit les dispositions que <le titulaire> s'engage à mettre en œuvre pour répondre aux exigences de sécurité des HCL. Il définit en particulier l’organisation qui sera mise en place, la méthodologie à suivre pour gérer la sécurité du projet d’externalisation et les mesures techniques, organisationnelles et procédurales qui seront mises en œuvre. Le candidat précisera le circuit d’approbation du Plan d’Assurance Sécurité, ses modalités d’application et l’étendue de sa diffusion.

# Document de référence

Ce paragraphe liste les documents de référence pour le Plan d’Assurance Sécurité. À titre d’exemple, les documents applicables peuvent être les suivants :

* le contrat ;
* le cahier des charges, incluant les exigences de sécurité des HCL ;
* le plan d’assurance qualité ;
* etc.

# Description du système

Ce paragraphe présente succinctement le système (ensemble des informations, logiciels, matériels et interfaces) concerné par les prestations. L’accent sera mis sur les points qui justifient la mise en œuvre de mesures de sécurité.

# Rappel des exigences générales de sécurité

Ce paragraphe fait référence, à minima, aux exigences techniques de la DSII.

# Rappel des exigences spécifiques de sécurité

Ce paragraphe reprend les exigences fonctionnelles de sécurité requise après classification des informations à traiter.

Le détail fonctionnel des classifications en fonction d’échelles relatives à la disponibilité, l’intégrité, la confidentialité et la traçabilité sont décrites en Annexe 1.

# Organisation

Ce paragraphe permet de décrire l’organisation que <le titulaire> propose pour gérer la sécurité des opérations.

On y trouve au minimum :

• le responsable du projet, agissant au nom des HCL ;

• <Le titulaire> ;

• les sous-traitants, cotraitants et fournisseurs de <le titulaire>.

Le rôle et éventuellement les modalités de participation à la gestion de la sécurité du projet de chacun sont décrits.

Ce paragraphe permet également de décrire l’organisation mise en place pour assurer les relations avec les HCL concernant les aspects de sécurité.

# Organisation de <le titulaire>

*En tant que responsable de la mise en œuvre, <le titulaire>, désignera un interlocuteur en charge de la sécurité.*

*Les missions du correspondant sécurité du projet peuvent être confiées au chef de projet selon la taille du projet.*

*Le correspondant sécurité pilote la sécurité des développements, du paramétrage, des prestations ainsi que la sécurité de la solution cible et de l’intégration des composants.*

*Le correspondant sécurité prend en charge la préparation d’un état des lieux de la sécurité du projet lors des comités de pilotage.*

*En comité de pilotage, il peut présenter les difficultés rencontrées pour satisfaire les exigences de sécurité de la solution. Il évoque éventuellement les incidents de sécurité en détaillant les impacts et les mesures prises pour éliminer ou diminuer la probabilité de récurrence.*

*De plus, il conseille les HCL dans son approche de la sécurité du projet, selon les audits, les incidents détectés ou les évolutions du contexte opérationnel.*

*Le correspondant sécurité du projet fait valider le PAS, s’assure de sa diffusion et vérifie que les moyens mis en œuvre correspondent aux exigences.*

# Organisation des HCL

*Les HCL désigneront un interlocuteur responsable de la sécurité du projet. Cet interlocuteur unique sera rattaché directement au directeur de projet.*

*Ce dernier a pour mission de faciliter les relations entre les différents intervenants et de mettre à disposition du titulaire l’ensemble des documents de sécurité nécessaires au bon déroulement du projet : politique de sécurité interne, documentation technique, spécifications, etc…*

*Il a également pour mission de s’assurer de la prise en compte globale de la sécurité par <le titulaire>.*

*Il décide de la conduite à tenir selon le résultat des audits, des incidents ou des conseils de <le titulaire>.*

*Il valide l’ensemble des actions réalisées au titre de la gestion de la sécurité du projet.*

# Responsabilités liées au Plan d’Assurance Sécurité

*Le titulaire, au travers de son responsable de la sécurité désigné, est responsable de la rédaction, de l’évolution et de la bonne exécution du PAS.*

*Il doit être approuvé par les HCL.*

*Il s’applique à l’ensemble des équipes lors de la mise en œuvre.*

*La cohérence de l’ensemble des mesures pourra être analysée et réévaluée lors des réunions d’avancement (ou revues de pilotage).*

# Procédure d’évolution

*Le titulaire est responsable de la rédaction du PAS initial et de ses évolutions pour répondre aux exigences de sécurité des Hospices Civils de Lyon pendant toute la durée du marché.*

*Voici une liste (non exhaustive) des situations susceptibles d’entraîner une modification du PAS :*

*• évolution du système d’information (configuration logicielle ou matérielle) ;*

*• évolution de l’environnement du système d’information (locaux, personnels, procédures, etc.) ;*

*• évolution du périmètre de service.*

*En cas d’évolution du système, de son environnement, ou du périmètre de service, le titulaire vérifie si le PAS doit être modifié. Si tel est le cas, il propose une modification aux HCL. Si cette modification est acceptée, le PAS est révisé, soumis aux HCL pour validation formelle et diffusé à l’ensemble des acteurs pour application.*

# Applicabilité

*Le PAS est applicable à l’ensemble des acteurs du projet, au même titre que le Plan d’Assurance Qualité, le cas échéant et avec la même priorité.*

*Un acteur du projet identifiant un non-respect du PAS dans ses procédures et mesures doit en référer immédiatement à <le titulaire>, qui en avertira les HCL. Un modèle type de rapport de non-respect sera annexé au PAS définitif, spécifiant la forme du rapport, la liste de diffusion, les responsabilités des acteurs, et le planning de traitement de la clause de non-respect.*

# Mesures de sécurité

Ce paragraphe permet de décrire les diverses clauses de sécurité qui couvrent les différentes typologies de projets ou sous projets. Il appartient à <le titulaire> de retenir les clauses pertinentes compte tenu du contexte, et d’en élargir leur portée si besoin.

## Ressources humaines

Ce paragraphe recueille l’engagement de <le titulaire> à :

• proposer des personnes dont le profil est en adéquation avec les missions confiées ;

• faire respecter à ses collaborateurs, ses sous-traitants, ses cotraitants ou ses fournisseurs concernés, l’ensemble des règles de sécurité des HCL via notamment la politique de sécurité du SI (PSSI) et ses procédures opérationnelles, la politique de sécurité du SI, etc.

## Transfert

Dans le cadre d’un projet d’externalisation par exemple, ce paragraphe décrit les mesures proposées pour sécuriser la phase de transfert du système.

Il s’agit notamment du transfert de matériels, des logiciels, des prestations, des procédures de contrôle de la sécurité du transfert, des obligations de restitution en comité de suivi sécurité, etc.

## Installation, exploitation

Ce paragraphe permet de présenter les mesures mises en place pour assurer la protection du système en réponse aux exigences identifiées par les HCL.

## Réversibilité

Ce paragraphe recueille l’engagement de <le titulaire> 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 les HCL, ou par un autre prestataire.

# Matrice de couverture des exigences spécifiques

Ce paragraphe décrit les mesures de sécurité techniques, procédurales et organisationnelles retenues pour répondre aux exigences spécifiques de sécurité décrites au paragraphe 6.

# Documentation de suivi

Ce paragraphe recueille l’engagement de <le titulaire> sur la fourniture d’un corpus documentaire relatif à la sécurité du projet et des informations traitées.

Ces documents pourront être les suivants :

|  |  |
| --- | --- |
| Nature du document :  PAS, version 1  PAS, version définitive  Dossier de sécurité  Plan de secours  Plan de gestion des incidents  Comptes-rendus de réunion du comité de suivi  Etc … | Date de remise :  Remise du dossier de réponse à consultation  Début de phase de transfert ou d’installation  Début de phase d’exploitation  Début de phase d’exploitation  Début de phase d’exploitation  Une semaine après chaque réunion  Etc … |

# Glossaire

|  |  |
| --- | --- |
| Terme | Description |
| PAS | Plan d’Assurance Sécurité |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Annexe 1 : Classification en sécurité

Au sein d’un système d’information, chaque information gérée peut avoir besoin de niveaux de sécurisations distincts en fonction des besoins respectifs de protection.

Une classification sur chacun des critères de sécurité : disponibilité, intégrité, confidentialité, traçabilité, conditionne les moyens de sécurisation à mettre en œuvre.

Les différentes échelles, issues de la PSSI des HCL, ainsi que les exigences fonctionnelles associées permettent d’apprécier la criticité du système à fournir et adapter les mesures au besoin de sécurisation.

**Échelle de confidentialité**

|  |  |  |
| --- | --- | --- |
| **Niveau** | | **Description Fonctionnelle** |
| C1 | Public | Diffusion libre quel que soit le lecteur |
| C2 | Restreint | Diffusion interne |
| C3 | Confidentiel | Diffusion limitée à un service ou une liste de destinataires |
| C4 | Secret | La nature des informations traitées (notamment les données de santé à caractère personnel) nécessite un accès limité à une liste nominative et restreinte de personnes, et une revue régulière des accès. Pour ce faire, il est recommandé de s’appuyer sur le système de gestion des identités et des habilitations déployé aux HCL.  La sécurité du transport doit également respecter les exigences de sécurité des données transportées. Le chiffrement des données échangées doit être assuré de bout en bout pour les données sensibles et en particulier pour toutes les données de santé à caractère personnel. |

**Échelle de disponibilité**

| **Niveau** | | **Exigence Fonctionnelle** |
| --- | --- | --- |
| D1 | faible | Ressource non nécessaire pour assurer une continuité métier |
| D2 | Important | Ressource ou information nécessitant la mise en place de processus ou de mécanismes assurant sa disponibilité. L’indisponibilité de la ressource ou de l’information est mesurable et tolérée pour une durée maximale de 1 jour ouvré. |
| D3 | Critique | Ressource ou information nécessitant la mise en place de processus ou de mécanismes assurant une haute disponibilité. Un mode de fonctionnement dégradé doit être mis en place dans un délai d'une heure maximum, le rétablissement devant intervenir dans un délai de 4 heures maximum 24H/24 5J/7 |
| D4 | Vital | Ressource ou information nécessitant la mise en place de processus ou de mécanismes assurant une très haute disponibilité. Un mode de fonctionnement dégradé doit être mis en place dans un délai de 1 heures maximum, le rétablissement complet du fonctionnement devant intervenir dans un délai de 4 heures maximum. |

**Échelle d’Intégrité**

|  |  |  |
| --- | --- | --- |
| **Niveau** | | **Exigence Fonctionnelle** |
| I1 | Faible | La donnée ne nécessite PAS de traçabilité réglementaire et n’intervient PAS dans les applications critiques ou sensibles .Le taux de mise à jour de la donnée est faible. |
| I2 | Important | La donnée a un faible taux de mise à jour, non critique pour les métiers, elle doit cependant être disponible. Les traces des accès en mise à jour ont une durée de conservation minimum d’un mois. |
| I3 | Critique | Tout accès en écriture aux données fait l’objet d’une trace complète (date, heure, utilisateur, origine) et conservée pendant la durée réglementaire en vigueur |
| I4 | Vital | Aucune perte ou corruption de données n’est admise.Tout accès en écriture aux données fait l’objet d’une trace complète (date, heure, utilisateur, origine) et conservée pendant la durée réglementaire en vigueur. |

**Échelle de Traçabilité**

| **Niveau** | | **Exigence Fonctionnelle** |
| --- | --- | --- |
| T1 | Faible | Les actions d’usage ne nécessitent PAS de traçabilité particulière |
| T2 | Nécessaire | Les actions d’usage font l’objet de traces |
| T3 | Essentielle | Les actions sont tracées aux fins d’analyse lors d’incidents impactant la disponibilité de la solution |
| T4 | Vitale | Les actions sur les données de santé à caractère personnel sont soumises à une disposition de traçabilité réglementée et opposable aux HCL.  Tout accès ou tentative d’accès aux données traitées par la solution doit être tracée et susceptible d’être transmise au patient à sa demande. Tout accès en écriture aux données fait l’objet d’une trace fonctionnelle complète. Elle consigne au minimum :   * le type d’action ; * la date et l’heure de l’action ; * l’identité de l’utilisateur et de la machine ayant effectué l’action ; * le résultat de l’action (succès, erreur, refus…) ; * le cas échéant, le lien vers les données métiers concernées et d’éventuelles traces embarquées (ex. identifiant de documents déposés).   Dans certains cas, ces éléments sont à compléter avec des informations de contexte, par exemple :   * l’historique des données métiers (ex. historique des versions de documents et préservation de l’intégrité de toutes les versions) ; * le contexte de réalisation de l’action, en particulier les informations fournies à l’utilisateur lui permettant d’évaluer la portée de son action (ex : message d’avertissement de l’utilisateur avant acquittement d’une alarme vitale). * le paramétrage technique de l’application.   L’accès aux fichiers de traces doit être géré de manière stricte et efficace. Seules les personnes dûment autorisées par la maîtrise d’ouvrage HCL doivent pouvoir y accéder en consultation. Elles ne peuvent être accessibles qu’aux professionnels de santé et aux personnels techniques sous la responsabilité de ces professionnels de santé, l’accès étant également limité à l’exercice strict de leur mission.  Aucune modification des traces ne doit être possible par la personne qui y accède. |