

## **ANNEXE 1**

### **PLAN ASSURANCE SECURITE**

PAS : 19 Version : 0.1

**ENGAGEMENT DU TITULAIRE:**

Le Titulaire s'engage à respecter les conditions de sécurité du présent Plan d'Assurance Sécurité. Pour s'engager, le Titulaire doit:

- Cocher la case devant chaque exigence de la Cnam.
- Présenter/décrire les mesures de sécurité techniques, procédurales ou organisationnelles retenues pour démontrer la conformité aux exigences stipulées par la Cnam. Si le Titulaire souhaite s'appuyer sur des documents pour répondre aux exigences il est nécessaire qu'il indique les références précises: le nom et la référence du document et les paragraphes concernés.
- Signer le PAS en version validée pour sa mise en application.

Les informations apportées dans ce document sont confidentielles, et seront traitées comme telles par les deux parties.

Date	Signature du Titulaire		
	Nom & prénom	Direction	Signature

## Plan Assurance Sécurité (PAS)

**Prestation de prise en charge des contacts entrants dans le cadre de  
déploiement généralisé du service « Mon espace santé »**

**Type de marché : Support-Télémaintenance  
PAS V0**

Etat	Nom	Service	Date
Rédaction			
Validation			

	Historique des modifications	
Version	Date	Objet

	Diffusion du document	
Date	Nom & prénom	Organisation

CNAM / DDSI	Plan Assurance Sécurité	4 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## SOMMAIRE

<b>1. PRESENTATION DU DOCUMENT .....</b>	<b>5</b>
1.1 INTRODUCTION.....	5
1.2 OBJECTIFS .....	5
1.3 RESPONSABILITES LIEES AU PAS.....	6
1.4 APPLICATION DU PAS .....	7
1.5 CAS DE NON-RESPECT ET DEROGATION DU PAS.....	8
<b>2. DESCRIPTION DE LA PRESTATION.....</b>	<b>9</b>
2.1 CONTEXTE ET OBJECTIFS .....	9
2.2 FONCTIONNALITES .....	9
2.3 BIENS SENSIBLES A PROTEGER.....	9
<b>3. REFERENCES DOCUMENTAIRES .....</b>	<b>10</b>
3.1 DOCUMENTS SECURITE .....	10
3.2 DOCUMENTS DU TITULAIRE.....	10
3.3 LIVRABLES SECURITE .....	10
<b>4. ORGANISATION SECURITE DE LA PRESTATION .....</b>	<b>11</b>
4.1 ORGANISATION DE LA CNAM ET CONTACTS SECURITE .....	11
4.2 ORGANISATION DU TITULAIRE ET CONTACTS SECURITE .....	11
4.3 INSTANCES DE SECURITE .....	12
4.4 INDICATEURS TABLEAU DE BORD SSI .....	12
<b>5. EXIGENCES DE SECURITE ET MESURES DE SECURITE MISES EN ŒUVRE .....</b>	<b>13</b>
5.1 ORGANISATION DE LA SECURITE (ORG) .....	14
5.2 GESTION DES ACTIFS ET MAITRISES DES RISQUES (CLA).....	16
5.3 GESTION DE CRISE SSI – CONTINUITE D’ACTIVITE (CRI).....	18
5.4 SECURITE LIEE AUX RESSOURCES HUMAINES (SRH) .....	19
5.5 SECURITE PHYSIQUE (SPH) .....	22
5.6 GESTION DE L'EXPLOITATION ET DES COMMUNICATIONS (GEC) .....	26
5.7 CONTROLE DE L'ACCES ET DES HABILITATIONS (CAH).....	35
5.8 SECURITE DU SUPPORT ET DE MAINTENANCE (SUP) .....	39
5.9 GESTION DES INCIDENTS (GDI).....	43
5.10 GESTION DES TIERS (GDT) .....	44
5.11 CONTROLE ET CONFORMITE (CTL).....	45
5.12 CONFORMITE (CFT).....	46
5.13 PHASE DE REVERSIBILITE (REV).....	47
<b>6. EXEMPLES D’INDICATEURS.....</b>	<b>48</b>

CNAM / DDSI	Plan Assurance Sécurité	5 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

# 1. PRESENTATION DU DOCUMENT

## 1.1 INTRODUCTION

Le présent document constitue le Plan d'Assurance Sécurité (PAS).

Il est entendu par « Assurance Sécurité » la garantie que la prestation se déroule dans les conditions de sécurité adaptées et garantisse un niveau d'assurance satisfaisant quant à la protection des données et des systèmes de la Cnam.

**Ce document décrit les exigences de sécurité de la Cnam et les dispositions que le Titulaire s'engage à mettre en œuvre pour y répondre.** Il définit en particulier l'organisation qui sera mise en place, la méthodologie à suivre pour gérer la sécurité de la prestation et les mesures techniques, organisationnelles et procédurales qui seront mises en œuvre.

## 1.2 OBJECTIFS

Ce document a pour objectif de:

- Fixer les responsabilités respectives entre la Cnam et le Titulaire en termes de sécurité ;
- Décrire les exigences sécurité de la Cnam ;
- Etablir les dispositions que le Titulaire s'engage à mettre en œuvre pour répondre aux exigences de sécurité émises par la Cnam.

CNAM / DDSI	Plan Assurance Sécurité	6 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

### 1.3 RESPONSABILITES LIEES AU PAS

Le présent document s'applique à l'ensemble du périmètre de la prestation. Le tableau ci-dessous décrit les responsabilités liées au présent document:

	Cnam	Titulaire
Fourniture des exigences de sécurité	X	
Description des réponses aux exigences		X
Évolution du document	X	X
Validation du document	X	
Diffusion du document	X	X

#### 1.3.1 Entrée en application du PAS

Le Titulaire est chargé d'élaborer le PAS par la description des mesures de sécurité qu'il propose de mettre en œuvre face aux exigences de la Cnam afin de garantir le respect des exigences de sécurité.

Le Titulaire doit:

- Décrire les dispositions de sécurité qu'il applique pour garantir la sécurité de réalisation de la prestation conformément aux exigences de sécurité définies par la Cnam.

**Remarque:** Pour toute disposition déjà en vigueur chez le Titulaire (car n'étant pas spécifique à la prestation), ce dernier peut simplement les mentionner dans le PAS et citer les documents qui les décrivent. Ces documents doivent pouvoir être consultés sur simple demande par la Cnam.

- Décrire les mesures qu'il met en place pour répercuter les exigences de sécurité de la Cnam vers tous ses sous-traitants et cotraitants.

La Cnam étudie les réponses du Titulaire faites dans le présent PAS et pourra demander des compléments d'informations ou précisions.

Le Titulaire est chargé de faire appliquer le PAS par les différents acteurs intervenant sur dans le cadre du marché(*collaborateurs du Titulaire, sous-traitants, cotraitants, partenaires, etc.*)

#### 1.3.2 Processus d'évolution du PAS

En début de marché, le Titulaire rédigera la version finale du PAS et le transmettra à la Cnam pour validation.

Le PAS fourni par le Titulaire au moment de la signature du marché deviendra une pièce contractuelle conformément à l'article <4.1>du CCAP du marché.

CNAM / DDSI	Plan Assurance Sécurité	7 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

Au cours de la prestation, des évolutions peuvent entraîner une révision du PAS, telles que:

- Une modification du système d'information ;
- Une modification de l'environnement du système d'information dans le périmètre de la prestation ;
- Une modification de l'organisation proposée par le Titulaire ;
- Une modification des exigences de la Cnam ;
- Une évolution du périmètre de la prestation ;
- Un incident de sécurité.

Les évolutions du PAS seront réalisées par le responsable ou le correspondant sécurité désigné par le Titulaire. La version révisée du PAS sera transmise à la Cnam pour validation formelle, et diffusée à l'ensemble des acteurs pour application. La validation formelle de la Cnam sera actée à l'occasion d'un comité de pilotage.

Il appartient au Titulaire de veiller à l'adéquation constante du PAS avec le niveau de sécurité attendu. Ainsi, toute évolution du PAS fera l'objet d'évaluation d'impact sécurité et devra être signalée à la Cnam. Elle sera accompagnée, si nécessaire par des actions correctives afin de rétablir le niveau de sécurité attendu.

Lorsqu'une mise à jour du PAS est rendue nécessaire, notamment, par l'évolution du cadre réglementaire, technique, applicatif, ou par une modification de la prestation, les éléments qui y sont décrits doivent être complétés ou mis à jour. De telles évolutions peuvent être à l'initiative de la Cnam ou du Titulaire. Elles doivent être soumises à la Cnam, qui peut les accepter ou les refuser.

Chaque évolution du PAS fera l'objet d'une évolution du numéro de version et sera tracée dans la fiche de suivi des versions du document.

## 1.4 APPLICATION DU PAS

### 1.4.1 Applicabilité du PAS

Le PAS est applicable à l'ensemble du périmètre de la prestation, il constitue un document contractuel lié à la prestation attendue par la Cnam.

Si l'une des parties constate un non-respect du PAS, il devra le faire savoir à l'autre partie dans les plus brefs délais.

### 1.4.2 Contrôle et suivi de l'application du PAS

Le Titulaire réalisera l'auto –évaluation de conformité aux exigences du PAS et transmettra à la Cnam un tableau de bord de suivi des mesures de sécurité à une fréquence à définir.

Ces tableaux de bord seront examinés lors des comités de pilotage de la prestation.

Le Titulaire s'engage à traiter tout point de la prestation identifiée comme étant en divergence avec le PAS, ou, plus généralement, en divergence avec les exigences de sécurité de la prestation et de façon adaptée à leur gravité. Ce traitement devra être formalisé sous la forme d'un plan d'actions proposé par le Titulaire, soumis à validation de la Cnam et annexé au PAS. Le suivi de l'avancement de ce plan d'actions sera intégré au suivi de la prestation.

CNAM / DDSI	Plan Assurance Sécurité	8 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## 1.5 CAS DE NON-RESPECT ET DEROGATION DU PAS

Tout non-respect du PAS doit être autorisé par la Cnam par le biais d'une dérogation formalisée.

La demande de dérogation doit être justifiée et soumise par le Responsable de la prestation à la personne responsable du marché à la Cnam.

La demande de dérogation ainsi notifiée devra être soumise à la validation du comité de pilotage qui statue sur une dérogation temporaire avec précision de la durée ou définitives. Si des divergences non autorisées avec le PAS sont mises en évidence, le Titulaire est tenu de définir un plan d'actions contenant des échéances, et de mettre en place ce plan d'actions. En cas de non-respect des échéances du plan d'actions ou en cas d'absence de plan d'actions, le Titulaire sera redevable du paiement de pénalités. Les modalités de calcul et d'application des pénalités sont précisées dans le CCAP du marché.

La Cnam se réserve le droit de suspendre les accès du Titulaire à son système d'information en cas de non-respect d'un ou plusieurs engagements du PAS.



CNAM / DDSI	Plan Assurance Sécurité	9 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## 2. DESCRIPTION DE LA PRESTATION

### 2.1 CONTEXTE ET OBJECTIFS

*Ce paragraphe présente le contexte et les objectifs du marché. Le Titulaire décrira brièvement le l'objet du marché et le périmètre macroscopique de celui-ci.*

### 2.2 FONCTIONNALITES

*Le Titulaire décrira brièvement les activités attendues, les principales fonctionnalités et les services fournis relevant du périmètre de la prestation.*

### 2.3 BIENS SENSIBLES A PROTEGER

*Le Titulaire présentera les données ou ressources sensibles entrant dans le périmètre de la prestation.*

*Pour cela, il peut par exemple être intéressant de se référer aux informations portées dans le dossier de sécurité, s'il existe, ou sur une analyse de risques propre au contexte du marché (mettant en relief les principaux risques à cadrer et les mesures associées).*

CNAM / DDSI	Plan Assurance Sécurité	10 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

### 3. REFERENCES DOCUMENTAIRES

*Sauf mention contraire, la dernière version validée du document cité ci-dessous est applicable.*

#### 3.1 DOCUMENTS SECURITE

Nom du document	Version

#### 3.2 DOCUMENTS DU TITULAIRE

Le Titulaire liste ci-dessous les documents de sécurité applicables au périmètre de la prestation:

Nom du document	Version

Le Titulaire précise ici les modalités de mise à disposition de ces documents:

Mise à disposition des documents

#### 3.3 LIVRABLES SECURITE

Le Titulaire liste ci-dessous l'ensemble de la documentation sécurité qu'il est amené à livrer dans le cadre de la prestation:

Type	Nom du document

CNAM / DDSI	Plan Assurance Sécurité	11 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## 4. ORGANISATION SECURITE DE LA PRESTATION

### 4.1 ORGANISATION DE LA CNAM ET CONTACTS SECURITE

La Cnam désignera un interlocuteur pour toute problématique de sécurité. D'autres interlocuteurs opérationnels pourront être ajoutés au cours de la prestation.

Un comité de pilotage devra se réunir une fois par an, sur la thématique de la « sécurité ». Les participants à ces réunions seront définis en accord avec la Cnam et le Titulaire.

L'interlocuteur de la sécurité désigné par la Cnam a pour mission de s'assurer de la prise en compte globale des clauses du présent PAS. Il décide de la conduite à tenir selon le résultat des audits, des incidents ou des conseils remontés par le Titulaire. Il valide l'ensemble des actions réalisées au titre de la gestion de la sécurité du marché. Le tableau ci-dessous définit les interlocuteurs de la Cnam:

Nom Prénom	Fonction	Coordonnées

### 4.2 ORGANISATION DU TITULAIRE ET CONTACTS SECURITE

Le Titulaire proposera une organisation pour gérer la sécurité tout au long du marché. Il attribuera notamment la responsabilité des sujets sécurité et désignera la personne qui fera office d'interlocuteur vis-à-vis de la Cnam.

Le Titulaire définit également les moyens de suivi des sujets sécurité (par exemple via un comité de suivi dédié ou l'intégration à un comité de pilotage), ainsi que le responsable de ces moyens de suivi (organisation, convocation, ordre du jour, comptes rendus).

Le responsable des sujets sécurité pourra conseiller la Cnam sur l'approche de la sécurité à adopter en fonction des audits réalisés, des incidents remontés ou évolutions du contexte opérationnel en cours d'exécution du marché.

Le Titulaire doit préciser ci-dessous quels sont les contacts sécurité au sein de son organisation:

Nom Prénom	Fonction	Coordonnées

CNAM / DDSI	Plan Assurance Sécurité	12 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

### 4.3 INSTANCES DE SECURITE

Des instances formelles de pilotage et de suivi de sécurité doivent être mise en œuvre lors du déroulement de la prestation entre la Cnam et le Titulaire.

Ces instances de pilotage de la sécurité peuvent simplement être adossée aux instances standards de suivi du marché avec dans l'ordre du jour le point spécifique à la sécurité.

<b>Nom du comité:</b> À compléter
<b>Participants:</b> À compléter
<b>Fréquence:</b> À compléter
<b>Objectifs:</b> À compléter
<b>Diffusion des comptes rendus:</b> À compléter

### 4.4 INDICATEURS TABLEAU DE BORD SSI

#### 4.4.1 Liste des indicateurs SSI

Les indicateurs devront refléter le niveau de sécurité atteint et permettre de maîtriser les risques liés à la prestation.

Les principaux indicateurs jugés nécessaires par la Cnam sont portés au chapitre 6 du présent document. Toutefois, le choix final des indicateurs pourra être soumis à une décision conjointe de la Cnam et du Titulaire.

Les indicateurs retenus seront définis lors de la tenue des premières instances de pilotage de la sécurité et consignés dans le tableau qui suit:

Chapitre	Indicateur
ORG	À compléter
CLA	À compléter
DIS	À compléter
SRH	À compléter
SPH	À compléter
GEC	À compléter
CAH	À compléter
DEM	À compléter
GDI	À compléter
GDT	À compléter
CTL	À compléter

#### 4.4.2 Modalités de suivi d'indicateurs

Le Titulaire est responsable de la remontée d'indicateurs vers le correspondant sécurité de la Cnam. Les comités de pilotage périodiques doivent consacrer un volet de sécurité permettant de présenter le tableau de bord des indicateurs pour analyse et proposer les mesures correctives si besoin est.

CNAM / DDSI	Plan Assurance Sécurité	13 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## 5. EXIGENCES DE SECURITE ET MESURES DE SECURITE MISES EN ŒUVRE

Ce chapitre fournit les exigences de sécurité qui s'appliqueront au Titulaire, ainsi que les mesures de sécurité que le Titulaire s'engage à mettre en œuvre dans le cadre de la prestation. Ces mesures sont destinées à garantir la sécurité de l'organisation pendant la phase de réalisation de la prestation.

Pour chaque exigence de ce chapitre, le Titulaire présentera les mesures de sécurité techniques, procédurales ou organisationnelles retenues pour répondre aux exigences de la Cnam.

CNAM / DDSI	Plan Assurance Sécurité	14 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## 5.1 ORGANISATION DE LA SECURITE (ORG)

### ORG-GOV Mise en place d'une organisation de la sécurité

#### Exigence de la Cnam:

Le Titulaire s'engage à mettre en place une organisation adéquate ayant pour objectif de gérer la gouvernance de la sécurité en lien avec la prestation

**ORG-GOV-01:** Le Titulaire doit décrire l'organisation de sécurité qu'il mettra en place. En particulier, le Titulaire précisera comment il prendra en compte le volet de sécurité dans les comités de gouvernance de la prestation (ex. la fréquence, participants, périmètre de suivi...). Au début du marché, ces modalités seront à valider conjointement avec la Cnam et à mettre en évidence au chapitre 4 du PAS.

**ORG-GOV-02:** En cas de cotraitance, il conviendra de préciser le périmètre de responsabilité et d'action incombant chaque cotraitant (ex. RACI).

**ORG-GOV-03:** Le Titulaire doit désigner parmi son personnel un correspondant de sécurité pour toute la durée de la prestation. Ce dernier doit être joignable aux horaires convenus dans le cadre contractuel. Tout remplacement de ce correspondant doit être notifié à la Cnam préalablement à son entrée en vigueur. De plus, une suppléance de ce correspondant de sécurité doit être assurée pour pallier son indisponibilité. Le correspondant de sécurité doit avoir un parcours et une expérience en sécurité des SI afin d'assurer les missions suivantes:

-l'interlocuteur privilégié de la Cnam pour toutes les questions relatives à la sécurité de la prestation, notamment dans le cadre d'investigations initiées par la Cnam ou le Titulaire suite à des incidents de sécurité opérationnels;

-le conseil et l'assistance dans la mise en œuvre des dispositifs de sécurité relatifs à prestation en vue d'optimiser la protection des données à chaque instant conformément au RGPD;

- le maintien, la mise en application du PAS, l'auto-évaluation de conformité des mesures de sécurités et du suivi des indicateurs de sécurité ;

- le contrôle d'efficacité des procédures et mesures de sécurité mises en place dans le cadre de la prestation et le suivi du plan d'action relatif aux éventuels audits déclenchés par le Titulaire ou la Cnam.

**Le Titulaire s'engage à respecter l'exigence et à mettre en œuvre les mesures de sécurité décrites ci-dessous: ☐Oui ☐Non**

*Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.*

CNAM / DDSI	Plan Assurance Sécurité	15 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## ORG-REF-DOC Référentiel de la documentation de la prestation

### Exigence de la Cnam:

Le Titulaire s'engage à formaliser, tenir à jour la documentation applicable à la prestation et mettre en place une gestion sécurisée de la documentation.

**ORG-REF-DOC-01:** Le Titulaire doit marquer systématique le niveau de confidentialité des documents en fonction de la classification des informations contenues.

**ORG-REF-DOC-02:** Le Titulaire doit mettre en place un mécanisme de gestion documentaire sécurisé permettant de se prémunir contre les accès non-autorisés.

**ORG-REF-DOC-03:** Le Titulaire doit réaliser les contrôles et filtrages nécessaires pour éviter toute fuite d'informations sensibles dans la documentation. La documentation ne doit contenir aucune donnée personnelle sensible, ni données de sécurité (ex. code secret d'authentification, clé de chiffrement, etc.) Le Titulaire décrira le circuit de contrôle et de validation de la documentation.

**Remarque:** Par défaut le niveau de sensibilité d'un document sera « confidentiel ».

**Le Titulaire s'engage à respecter l'exigence et à mettre en œuvre les mesures de sécurité décrites ci-dessous: ☐Oui ☐Non**

*Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.*

CNAM / DDSI	Plan Assurance Sécurité	16 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## 5.2 GESTION DES ACTIFS ET MAITRISES DES RISQUES (CLA)

CLA-DON	Gestion des données et des ressources informatiques relatives à la prestation
<p><b>Exigence de la Cnam:</b></p> <p>Dans une démarche de prévention, de détection des risques, et de réaction efficace aux incidents de sécurité, le Titulaire s'engage à établir en début du marché et maintenir à jour un inventaire des informations, de leurs finalités et moyens de traitement associés (ressource informatiques matériels, logiciels, support de stockage...), à savoir:</p> <ul style="list-style-type: none"> <li>- celles qui lui sont confiées par la Cnam,</li> <li>- celles qu'il produit au titre de la prestation,</li> <li>- celles qu'il utilise pour réaliser la prestation.</li> </ul> <p><b>CLA-DON-01:</b> Le Titulaire est tenu de mettre à disposition de la Cnam et tenir à jour cet inventaire en s'appuyant sur un outillage adapté qui peut être un outil de gestion de configuration ou équivalent.</p> <p><b>CLA-DON-02:</b> Le Titulaire doit définir conjointement avec la Cnam les responsabilités appropriées en matière de traitement et de protection des informations par exemple la tenue d'un registre des données qui sont accessibles pour réaliser l'ensemble des prestations associés au marché.</p> <p><b>CLA-DON-03:</b> Le Titulaire doit évaluer conjointement avec la Cnam le niveau de sensibilité des informations et de leurs moyens de traitement associés en vue d'assurer la cohérence de protection.</p> <p><b>CLA-DON-04:</b> Le Titulaire doit marquer systématiquement le niveau de classification des informations et leurs moyens de traitements associés.</p> <p><b>CLA-DON-05:</b> Le Titulaire doit informer son personnel du niveau de la classification des données utilisées dans le cadre de la prestation et mettre à disposition de son personnel les moyens de protection associés.</p> <p><b>Remarque:</b> Par défaut le niveau de sensibilité d'information sera « confidentiel »</p>	
<p><b>Le Titulaire s'engage à respecter l'exigence et à mettre en œuvre les mesures de sécurité décrites ci-dessous:</b> <input type="checkbox"/>Oui <input type="checkbox"/>Non</p>	
<p><i>Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.</i></p>	



CNAM / DDSI	Plan Assurance Sécurité	17 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

#### CLA-EXT Utilisation des actifs et des informations en dehors de la prestation

##### Exigence de la Cnam:

**CLA-EXT-1:** Le Titulaire se porte garant de l'intégrité et de la confidentialité des actifs et informations de la Cnam auxquels il sera amené à avoir accès pendant l'exécution du marché.

**CLA-EXT-2:** Le Titulaire s'interdit:

- D'accéder à d'autres ressources, données, serveurs, informations ou documents de la Cnam que ceux faisant l'objet du marché. En particulier, il s'engage à ne pas accéder en direct ou par rebond à d'autres machines que celles nécessaires à la prestation.
- De copier des données sans autorisation expresse de la Cnam. En particulier, il s'engage à ne pas activer des moyens périphériques (clé usb, disques durs externes, téléphone portable, graveur, etc) pour exfiltrer les données.
- D'utiliser les données et informations en lien avec la prestation, en dehors de celle-ci. Cette exigence s'applique pendant toute la durée de la prestation ou de la garantie, ainsi qu'après la fin de la prestation.

**Le Titulaire s'engage à respecter l'exigence: ☐Oui ☐Non**

*Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.*

CNAM / DDSI	Plan Assurance Sécurité	18 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

### 5.3 GESTION DE CRISE SSI – CONTINUITE D’ACTIVITE (CRI)

CRI-SSI	Gestion de crise SSI
	<p><b>Exigence de la Cnam :</b></p> <p>Le Titulaire s’engage à mettre en œuvre, par anticipation, tous les dispositifs nécessaires pour gérer une crise liée à la sécurité sur le périmètre SI de la prestation sous sa responsabilité.</p> <p><b>CRI-SSI-01:</b> Le Titulaire doit disposer d'un plan de gestion de crise formalisé et opérationnel tenant en compte les aspects de la sécurité du SI.</p> <p><b>CRI-SSI-02:</b> Le plan de gestion de crise doit préciser au minimum:</p> <ul style="list-style-type: none"> <li>-les principes d'escalade (critère de déclenchement, synoptique d'escalade)</li> <li>-la composition de la cellule de crise (la liste nominative des acteurs concernés, de leurs suppléants, leurs coordonnées),</li> <li>- les fonctions et la responsabilité des membres de la cellule de crise (ex. responsabilité Titulaire, responsabilité Cnam, partage de responsabilité)</li> <li>-les moyens dédiés à la gestion de crise (ex. procédure et moyens de communication)</li> </ul> <p><b>CRI-SSI-03:</b> Le plan de gestion de crise Sécurité doit être revu et validé conjointement par le Titulaire et la Cnam.</p>
	<p><b>Le Titulaire s’engage à respecter l’exigence et à mettre en œuvre les mesures de sécurité décrites ci-dessous: <input type="checkbox"/>Oui <input type="checkbox"/>Non</b></p>
	<p><i>Le Titulaire décrit ici les moyens qu’il s’engage à mettre en œuvre pour le respect de l’exigence formulée par la Cnam.</i></p>

CNAM / DDSI	Plan Assurance Sécurité	19 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

#### CRI-SEC-PCA

#### Sécurité des données dans le Plan de Continuité d'Activités

##### Exigence de la Cnam :

Le Titulaire s'engage à mettre en œuvre, par anticipation, tous les dispositifs nécessaires pour gérer la sécurité des données et les traitements associés dans des situations défavorables, comme lors d'une crise ou sinistre majeur.

**CRI-SEC-PCA-01:** La continuité de la sécurité des données doit faire partie intégrante du plan de Gestion de la Continuité d'Activités selon les spécifications stipulées par le CCTP.

**CRI-SEC-PCA-02:** Le Titulaire doit disposer d'un plan de Gestion de la Continuité d'Activités formalisé et opérationnel dans le cadre de la prestation. Celui-ci doit préciser les modalités de maintien en condition opérationnelle de la sécurité des données, par exemple:

- le périmètre de couverture sous sa responsabilité
- le niveau de continuité de services fournis en conformité avec les besoins de la Cnam (PDMA Perte de Données Maximale Admissible, DIMA Durée d'Indisponibilité Maximale Admissible)
- les scénarios de sinistre pris en compte.
- la mise en œuvre des solutions de redondance et des procédures opérationnelles de secours, de sauvegarde et de restauration des données.
- la protection de la disponibilité, la confidentialité et l'intégrité des sauvegardes selon les modalités spécifiées par l'exigence GEC-SAU.

**Le Titulaire s'engage à respecter l'exigence et à mettre en œuvre les mesures de sécurité décrites ci-dessous: ☐ Oui ☐ Non**

*Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.*

## 5.4 SECURITE LIEE AUX RESSOURCES HUMAINES (SRH)

#### SRH-PER-CONF

#### Gestion du personnel intervenant dans le cadre de la prestation

##### Exigence de la Cnam :

Le Titulaire s'engage à s'assurer que le personnel intervenant dans le cadre de la prestation soit des salariés de confiance pour lutter contre les incidents de sécurité liés à la malveillance interne.

**SRH-PER-CONF-01:** Le Titulaire doit mettre en place le processus de gestion des mouvements de son personnel (arrivé, départ, changement dans les rôles et/ou responsabilités) intervenant dans le cadre de la prestation.

**SRH-PER-CONF-02:** Le Titulaire doit maîtriser l'inventaire de son personnel qui est intervenu à un instant donné sur la prestation quel que soit le lieu d'exécution (sur un site de la Cnam ou hors site). Il est tenu de réaliser un suivi périodique du personnel intervenant sur le SI de l'Assurance Maladie dans le cadre du marché. Toute entrée et toute sortie de personnel disposant d'accès au SI de l'Assurance Maladie doit

CNAM / DDSI	Plan Assurance Sécurité	20 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

être signalée à la Cnam afin de procéder à la gestion d'habilitation, de comptes d'accès (création, suppression, etc), d'attribution et du retrait de matériel mis à disposition.

**SRH-PER-CONF-03:** Le Titulaire est tenu de faire signer à tous les agissants en son nom ou pour son compte, une clause de confidentialité qui garantit le respect du cadre réglementaire et légal de la protection des données à caractère personnel ainsi que la protection des données confidentielles de la Cnam.

**SRH-PER-CONF-04:** Lors de l'intervention sur un site de la Cnam, le Titulaire est tenu de porter à connaissance et de faire signer à son personnel intervenant la charte de la Cnam et/ou le livret sécurité prestataire. Le Titulaire tiendra à jour la liste des signataires de ce(s) document(s).

**SRH-PER-CONF-05:** Le Titulaire est tenu de mettre en place un processus disciplinaire pour prendre des mesures à l'encontre des salariés ayant enfreint les règles de sécurité de la prestation.

**Le Titulaire s'engage à respecter l'exigence et à mettre en œuvre les mesures de sécurité décrites ci-dessous: ☐Oui ☐Non**

*Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.*

CNAM / DDSI	Plan Assurance Sécurité	21 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## SRH-SEN-FOR Sensibilisation et Formation du personnel à la sécurité

### Exigence de la Cnam :

Le Titulaire s'engage à ce que chacun des intervenants sous sa responsabilité dans le périmètre de la prestation soit formé des bonnes pratiques de sécurité en lien avec les métiers exercés et respecte les règles de protection du Système d'Information de la Cnam pour éviter les incidents de sécurité liés l'erreur humaine

**SRH-SEN-FOR-01:** Le Titulaire doit garantir un niveau adéquat de formation du personnel intervenant sous sa responsabilité. En particulier, il précisera les mesures prises pour assurer un niveau de formation en sécurité adapté aux missions de chacun.

**SRH-SEN-FOR-02:** le Titulaire doit établir et maintenir un processus documenté de sensibilisation à la sécurité de tout son personnel en lien avec la prestation. En complément, le Titulaire veille à ce que ses intervenants respectent les dispositions concernant la sécurité telles que décrites au Contrat et au présent PAS. Notamment:

- L'organisation sécurité de la prestation ;
- Les objectifs, rôles et responsabilités individuels ;
- Les procédures de sécurité liées à la prestation ;
- Les règles définies dans la charte de la Cnam et/ou dans le livret prestataire ;
- La protection du patrimoine informationnel de la Cnam ;
- Le respect de la confidentialité tel que défini au contrat ;
- Le signalement des incidents de sécurité ou des suspicions d'incidents de sécurité.

**SRH-SEN-FOR-03:** La sensibilisation doit être réalisée à la prise de poste du personnel du Titulaire sur le périmètre de la Prestation, puis annuellement ou en cas d'évolution des règles de protection du système d'information de Cnam ou en cas d'incident de sécurité majeur.

**Remarque:** La Cnam pourra planifier et organiser avec le Titulaire des sessions de sensibilisation aux enjeux métiers.

**Le Titulaire s'engage à respecter l'exigence et à mettre en œuvre les mesures de sécurité décrites ci-dessous: ☐Oui ☐Non**

*Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.*

CNAM / DDSI	Plan Assurance Sécurité	22 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## 5.5 SECURITE PHYSIQUE (SPH)

### SPH-BAT Accès physique aux bâtiments

#### Exigence de la Cnam :

Les accès physiques aux locaux du Titulaire hébergeant le personnel et/ou les ressources informatiques dans le cadre la prestation doivent être restreints aux seules personnes autorisées par des dispositifs de contrôle d'accès et de surveillance adéquats à l'entrée et à la sortie pour éviter toute intrusion physique.

**SPH-BAT-01:** Le Titulaire doit formaliser une politique de gestion des accès physiques aux locaux. Celle-ci doit préciser au minimum les modalités suivantes:

- le contrôle d'accès nominatif,
- la traçabilité des accès et sauvegarde des traces avec les informations sur l'identification, l'horodatage.
- la gestion des accès visiteurs,
- le découpage des sites ou locaux en zone de sécurité selon le niveau de sensibilité (i.e. espace de travail, centre de production, zone d'accueil). Pour chaque zone de sécurité, des critères précis d'authentification et d'autorisation d'accès doivent être établis.
- La surveillance et détection des intrusions

**SPH-BAT-02:** Le Titulaire doit préciser les moyens mis en œuvre pour faire appliquer sa politique de gestion de contrôle d'accès physiques.

**SPH-BAT-34 :** Les agents réalisant le support doivent être regroupés sur des plateaux ou des bureaux dédiés à l'activité objet du marché. L'accès à ces plateaux ou bureaux doit faire l'objet d'un contrôle d'accès strict. Le télétravail est autorisé à condition que le Titulaire sécurise les postes de travail et l'environnement de travail de ses collaborateurs.

**Le Titulaire s'engage à respecter l'exigence et à mettre en œuvre les mesures de sécurité décrites ci-dessous: ☐Oui ☐Non**

*Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.*

CNAM / DDSI	Plan Assurance Sécurité	23 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## SPH-EQU Equipements d'infrastructures et ressources informatiques

### Exigence de la Cnam :

Le Titulaire s'engage à protéger les équipements d'infrastructure et ressources informatiques utilisées dans le cadre de prestation (ex. infrastructure de la plateforme de télédiagnostic) contre les menaces environnementales (dégradation, endommagement, perte, vol, coupure de courant) portant atteinte à la continuité des activités et/ou des services offerts.

**SPH-EQU-01:** Les équipements d'infrastructures (ex. équipement réseau, serveurs) du Titulaire mis en place dans le cadre de l'exécution des prestations doivent disposer de mesures de protection adaptées, à savoir:

- Une sécurité d'alimentation électrique;
- Une surveillance climatisation ;
- Une sécurité incendie ;
- Une surveillance vidéo avec alerte de sécurité, et détection d'intrusion ;
- Une isolation des éléments ayant besoin d'une protection spéciale (zone de sécurité).

**SPH-EQU-02:** Les postes de travail du Titulaire utilisés dans le cadre de l'exécution des prestations doivent disposer de mesures de protection adaptées pour se prémunir contre le vol, la perte entraînant la fuite des données. Le Titulaire doit mettre en place à minimales mécanismes suivants:

- câble de sécurité antivol systématique,
- chiffrement du support de stockage, si possible par une solution de chiffrement qualifiée.

**SPH-EQU-03:** Le Titulaire doit mettre en place la maintenance préventive des matériels d'infrastructure et les ressources informatique qui concourent à la sécurité et à la continuité des opérations de la prestation.

**SPH-EQU-04 :** Le Titulaire doit soumettre à la Cnam et mettre en œuvre une solution interne qui permettra à la Cnam de vérifier que les postes utilisés dans le cadre du marché font l'objet d'un contrôle de conformité. Le rapport de conformité des postes doit remonter à une fréquence hebdomadaire auprès d'Atos Groupement.

**Le Titulaire s'engage à respecter l'exigence et à mettre en œuvre les mesures de sécurité décrites ci-dessous: ☐Oui ☐Non**

*Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.*

CNAM / DDSI	Plan Assurance Sécurité	24 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## SPH-INFO Protection de l'information sur support papier ou physique

### Exigence de la Cnam :

Le Titulaire s'engage à mettre en œuvre tous les moyens nécessaires à la protection des informations confidentielles disponibles sur supports papier ou physiques contre un accès non-autorisé, une utilisation frauduleuse ou une altération des informations.

**SPH-INFO-01:** Lorsque l'information confidentielle est utilisée, qu'elle soit sous format papier ou sur un support de stockage amovible, le Titulaire doit la mettre sous clé (de préférence dans un coffre –fort, armoire à clé ou équivalent).

**SPH-INFO-02:** Les impressions d'informations sensibles doivent être effectuées sous surveillance de l'utilisateur ou via un dispositif garantissant le contrôle de l'utilisateur, du déclenchement de l'impression jusqu'à la récupération du support imprimé (par exemple imprimante avec le mécanisme d'authentification par code ou badge).

**SPH-INFO-03:** En cas d'utilisation des imprimantes et copieurs multifonction dans le cadre de la prestation, le Titulaire s'interdit de les interconnecter avec un environnement externe non maîtrisé.

**Le Titulaire s'engage à respecter l'exigence et à mettre en œuvre les mesures de sécurité décrites ci-dessous: ☐Oui ☐Non**

*Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.*



CNAM / DDSI	Plan Assurance Sécurité	25 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## SPH-DECOM

## Mise au rebut ou recyclage sécurisé (e) des matériels

### Exigence de la Cnam :

Le Titulaire s'engage à mettre en œuvre des procédures et des moyens conformes aux règles de l'art (\*), pour lutter contre les incidents pouvant affecter la confidentialité des données lors du transfert, de la mise au rebut, ou du recyclage de tous supports, matériels de stockage intervenant dans le cadre de la prestation pour la Cnam.

**SPH-DECOM-01:** Le Titulaire doit formaliser les procédures d'effacement de données et de destruction des supports et matériels de stockage. En particulier, dans le cas de stockage de matériel en attente de traitement, les procédures doivent prendre en compte la protection physique du lieu de stockage.

**SPH-DECOM-02:** Le Titulaire doit préciser les mécanismes d'effacement sécurisé (de préférence des outils qualifiés par l'ANSSI ou équivalents) et de destruction des supports, matériels de stockage des données.

**SPH-DECOM-03:** Le Titulaire doit établir une fiche d'intervention à destination du responsable de la gestion des matériels de la Cnam, pour tracer au minimum des informations suivantes pour les matériels d'infrastructure de stockage:

- Identification du matériel (numéro de série, adresse mac ...);
- Date de transfert de l'équipement;
- Date et nature de l'intervention d'effacement ou de destruction effectuée ou transfert pour maintenance;
- Statut des opérations réalisées (opérateur, date, type d'effacement, contrôle de l'effacement, PV destruction...).

(\*) Les techniques d'effacement sécurisé des supports de stockage diffèrent en fonction de la technologie du support de stockage. Il convient de revoir les outils d'effacement pour s'assurer qu'ils sont applicables à la technologie du support de stockage considéré.

**Le Titulaire s'engage à respecter l'exigence et à mettre en œuvre les mesures de sécurité décrites ci-dessous: ☐Oui☐Non**

*Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.*

CNAM / DDSI	Plan Assurance Sécurité	26 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## 5.6 GESTION DE L'EXPLOITATION ET DES COMMUNICATIONS (GEC)

### GEC-DON Traitement et stockage des données

#### Exigence de la Cnam :

Le Titulaire s'engage à mettre en œuvre tous les moyens nécessaires pour assurer de bout en bout l'intégrité, la confidentialité du traitement et du stockage des données de la Cnam. Dans le contexte de la prestation, les données et les traitements doivent être établis conjointement avec la Cnam et mentionnés en ANNEXE-Registre des données et finalités de traitement associées (cf. CLA-DON).

**GEC-DON-01:** Le Titulaire doit garantir que le traitement et le stockage des données liées à la prestation Cnam soient cloisonnés vis-à-vis de ses propres données ou de données d'autres clients en vue de réduire tout risque d'interférence, d'interception, et détournement (utilisation frauduleuse) par un tiers malveillant.

**GEC-DON-02:** Pour les applications ou outils hébergeant les données de la Cnam (ex. outil Télédiagnostic, outil Support pour la gestion et suivi d'incident,...), le Titulaire doit préciser les composants dédiés à la Cnam, des composants mutualisés, les technologies (ou les mécanismes) de cloisonnement au travers d'un dossier d'architecture. Il convient que le dossier d'architecture indique à minima les différents niveaux de cloisonnement, par exemple physique, logique, accès, applicatif, système, base de données.

**GEC-DON-03:** En fonction de la technologie (ex. Virtualisation) utilisée, le Titulaire doit effectuer un durcissement et une revue périodique des configurations du système d'Hypervision (ou équivalent) pour assurer le maintien du cloisonnement traitement et de stockage des données pendant la durée de la prestation.

**GEC-DON-04:** Le Titulaire doit effectuer l'effacement ou suppression des données après un délai de conservation autorisé par la Cnam. Le Titulaire précise les moyens mis en œuvre afin de garantir la suppression ou l'effacement sécurisé (\*) des données et il est tenu de fournir à la Cnam la preuve de suppression ou effacement de ces données.

(\*) Les techniques d'effacement sécurisé des supports de stockage diffèrent en fonction de la technologie du support de stockage. Il convient d'utiliser les outils d'effacement conforme aux règles de l'art pour s'assurer qu'ils sont applicables à la technologie du support de stockage considéré.

**Le Titulaire s'engage à respecter l'exigence et à mettre en œuvre les mesures de sécurité décrites ci-dessous: ☐Oui ☐Non**

*Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.*

CNAM / DDSI	Plan Assurance Sécurité	27 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## GEC-SAU Sauvegarde et restauration des données de la prestation

### Exigence de la Cnam :

Le Titulaire s'engage à réaliser des copies de sauvegarde de l'information, des logiciels et des images systèmes, et de les tester régulièrement conformément à une politique de sauvegarde et restauration respectant à minima les principes directeurs suivants:

**GEC-SAU-1:** Le Titulaire doit protéger le stockage et contrôler l'accès au support de sauvegardes en vue d'éviter tout accès non-autorisé. Les supports de sauvegarde doivent être protégés en fonction du niveau de classification des informations qu'ils renferment.

**GEC-SAU-2:** Le Titulaire doit tester régulièrement les supports de sauvegarde pour s'assurer qu'il est possible de s'en servir, le cas échéant, en situation d'urgence.

**GEC-SAU-3:** Le Titulaire doit formaliser de manière exhaustive les modalités relatives aux plans de sauvegarde et de restauration des données, ressources informatiques (logiciel, système...) utilisées dans la prestation:

- Périmètre, nature et fréquence des sauvegardes,
- Tests de restauration et fréquence,
- Temps de récupération et restauration des données adaptés aux besoins de la prestation.

**Le Titulaire s'engage à respecter l'exigence et à mettre en œuvre les mesures de sécurité décrites ci-dessous: ☐Oui ☐Non**

*Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.*

CNAM / DDSI	Plan Assurance Sécurité	28 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## GEC-INT Interconnexion et échanges des données

### Exigence de la Cnam :

Toutes les demandes de connexion au SI de l'Assurance Maladie devront être validées par la Cnam. La demande devra notamment préciser le besoin, les ressources accédées, le lieu depuis lequel la connexion sera faite, les horaires d'accès, la période pendant laquelle le Titulaire a besoin de se connecter (date de début et date de fin).

**GEC-INT-01:** Le Titulaire est tenu de mettre en œuvre un seul point d'interconnexion entre son SI et celui de l'Assurance Maladie permettant d'assurer la confidentialité et l'intégrité des flux échanger des flux. Une connexion de type VPN IPsec sera à privilégier.

Le Titulaire est de plus tenu de:

- Ne pas accéder au SI de l'Assurance Maladie en dehors de ses locaux ou sites définis contractuellement. Les besoins de type «accès nomade» seront traités par exception et au cas par cas avec l'accord de la Cnam ;
- Ne pas accéder au Si de l'Assurance Maladie en dehors du cadre stricte de la prestation ;

**GEC-INT-02:** Le Titulaire doit préciser les mesures de contrôle et filtrage des flux dans le cadre des connexions pour autoriser uniquement les flux nécessaires aux activités de la prestation notamment:

- Pour accéder au SI de l'Assurance Maladie depuis son site
- Pour accéder au SI de l'Assurance Maladie depuis le site d'éventuel cotraitant (ou sous-traitant)

Ce dispositif peut être basé sur le filtrage des adresses IP, des protocoles, des ports associés aux flux via une passerelle sécurisée (ex. pare-feu, routeur-filtrant).

**GEC-INT-03:** Le Titulaire doit mettre en place les mécanismes de chiffrement lors des échanges des données confidentielles (de point à point) selon l'état de l'art et les mécanismes d'authentification des partenaires pour éviter l'interception et la manipulation des données par un tiers malveillant. Le Titulaire doit préciser les mécanismes de chiffrement & authentification des flux d'échanges de données. Par exemple, il convient de privilégier des protocoles de transport sécurisés basés sur TLS v1.2, avec authentification du client, ou authentification mutuelle des partenaires à base de certificatx509.

**GEC-INT-04:** Le Titulaire doit établir et tenir à jour le dossier d'architecture d'interconnexion et la matrice de flux d'échanges des données entre son SI et celui de l'Assurance Maladie en détaillant la fonctionnalité des flux et les mécanismes de sécurisation stipulées au-dessus.

**Le Titulaire s'engage à respecter l'exigence et à mettre en œuvre les mesures de sécurité décrites ci-dessous: ☐Oui ☐Non**

*Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.*

CNAM / DDSI	Plan Assurance Sécurité	29 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## GEC-CLO Cloisonnement des réseaux

### Exigence de la Cnam :

Le Titulaire est tenu de s'assurer du bon cloisonnement réseau des plateformes informatiques utilisées dans le cadre de la prestation afin de minimiser l'impact et la propagation d'une attaque provenant d'autres plateformes informatiques (ex. réseau d'utilisateurs, ou d'autres clients)

**GEC-CLO-01:** Le Titulaire doit mettre en place la gestion sécurisée des réseaux qui consiste à diviser en domaines de réseaux séparés selon le niveau de sensibilité. Le cloisonnement du réseau, où se trouvent les plates-formes utilisées dans le cadre de la prestation, peut être réalisé en utilisant un réseau physique ou un réseau logique.

**GEC-CLO-02:** Le Titulaire doit préciser les mécanismes de cloisonnement réseau où se trouvent les plates-formes utilisées dans le cadre de la prestation par rapport au reste de son système d'information. En cas de mutualisation avec d'autres plateformes informatiques, il doit mentionner également les éléments mutualisés et ceux qui ne le sont pas.

**GEC-CLO-03:** Le Titulaire doit formaliser les différents niveaux de cloisonnement de réseau à travers d'un dossier d'architecture et le tenir à jour au fil des évolutions apportées aux plates-formes informatiques utilisées dans le cadre de la prestation.

**Le Titulaire s'engage à respecter l'exigence et à mettre en œuvre les mesures de sécurité décrites ci-dessous: ☐Oui ☐Non**

*Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.*

CNAM / DDSI	Plan Assurance Sécurité	30 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## GEC-ATQ-RES Protection contre les attaques réseaux

### Exigence de la Cnam :

Le Titulaire s'engage à mettre en œuvre tous les moyens nécessaires pour se protéger contre les attaques classiques sur les réseaux (utilisés dans le cadre de la prestation) portant atteinte à la sécurité des activités liées à la prestation, à savoir:

- Déni de service réseaux (ex. syn flooding, déni de service distribués),
- Redirection de trafic réseaux,
- Usurpation d'adresse IP des équipements réseaux, serveurs, poste de travaux.

**GEC-ATQ-RES-1:** Le Titulaire doit durcir les configurations des équipements de réseaux (ex : le changement des mots de passe et certificats, la désactivation des interfaces et services inutiles)

**GEC-ATQ-RES-2:** Le Titulaire doit réaliser la surveillance l'état de sécurité des réseaux et la revue de configuration en vue de détecter toute vulnérabilité et/ou intrusion, via des solutions de types sondes de détection ou de prévention d'intrusion.

**Le Titulaire s'engage à respecter l'exigence et à mettre en œuvre les mesures de sécurité décrites ci-dessous: ☐Oui ☐Non**

*Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.*

CNAM / DDSI	Plan Assurance Sécurité	31 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## GEC-ANT Protection contre les codes malveillants

### Exigence de la Cnam :

Le Titulaire s'engage à mettre en place des logiciels de protection contre les codes malveillants (appelés communément antivirus en environnement Windows, anti-rootkit en environnement Unix/Linux) sur l'ensemble des serveurs d'interconnexion, serveurs applicatifs et postes de travail (ex. poste du mainteneur) utilisés dans le cadre de la prestation.

**GEC-ANT-01:** Cet outil de protection contre les codes malveillants doit fonctionner en permanence, depuis le démarrage des équipements informatiques jusqu'à leur arrêt. En cas d'arrêt volontaire ou accidentel de l'outil, il doit pouvoir être relancé automatiquement. La désactivation, même temporaire, d'un antivirus utilisé dans le cadre de la prestation devra avoir été préalablement validée par la Cnam.

**GEC-ANT-02:** En cas de détection d'un code malveillant par cet outil, une stratégie d'éradication définie doit être appliquée. De plus, en cas d'infection avérée d'un environnement dédié à la prestation, le Titulaire est tenu d'en informer la Cnam dans les plus brefs délais. Le Titulaire doit également informer la Cnam si un vecteur de propagation de l'infection depuis son SI vers le SI de l'Assurance Maladie a été identifié.

**GEC-ANT-03:** Le Titulaire doit préciser le(s) logiciel(s) pour la protection contre les codes malveillants. Il conviendra que ces outils soient distincts sur les serveurs et les postes de travail en vue de garantir une efficacité de protection maximale.

**GEC-ANT-04:** Le Titulaire doit effectuer un suivi périodique (au moins hebdomadaire) de la mise à jour des signatures antivirales des postes de travail et serveurs utilisés dans le cadre de la prestation. Les opérations de mise à jour doivent être les plus automatisées possibles afin de respecter au mieux les exigences de réactivité requises pour une protection efficace.

**GEC-ANT-05:** Le Titulaire doit effectuer une revue périodique des événements de sécurité provenant des outils de protection des doivent pour analyse et gestion des problèmes a posteriori (exemples: serveur constamment infecté, virus détecté et non éradiqué par l'antivirus, etc.)

**GEC-ANT-06:** L'accès au compte « administrateur local » sur les postes de travail utilisés dans le cadre de la prestation doit être strictement limité aux équipes en charge de l'exploitation et du support sur ces postes de travail pour éviter la désactivation de l'antivirus, ou installations d'un logiciel vérolé par un utilisateur.

**Le Titulaire s'engage à respecter l'exigence et à mettre en œuvre les mesures de sécurité décrites ci-dessous: ☐ Oui ☐ Non**

*Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.*

CNAM / DDSI	Plan Assurance Sécurité	32 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## GEC-ADM Sécurisation des actions d'administration

### Exigence de la Cnam :

Le Titulaire s'engage à s'assurer de la sécurisation des opérations d'administration, qui peuvent être:

- Administration des connexions et accès au SI de la Cnam et/ou à des services et données de la Cnam hébergés chez le Titulaire
- Administration des comptes utilisateurs et leurs attributs de sécurité
- Administration des infrastructures (ex. équipements, réseaux, systèmes...).

La sécurisation des opérations d'administration doit s'appuyer à minima sur les principes directeurs et moyens ci-dessous:

**GEC-ADM-01:** Le Titulaire doit tracer les opérations d'administration de manière à pouvoir gérer au niveau individuel l'imputabilité des actions d'administration

**GEC-ADM-02:** Les comptes et les privilèges d'accès « administrateur » doivent être utilisés uniquement pour les actions d'administration le nécessitant.

**GEC-ADM-03:** L'habilitation des administrateurs doit s'effectuer selon une procédure d'autorisation formelle (cf. voir les exigences CAH-GAH). L'accès aux outils et interfaces d'administration doit être strictement limité aux personnes habilitées.

**GEC-ADM-04:** Les flux d'administration doivent être authentifiés et chiffrés avec les mécanismes robustes(cf. GEC-CRYPT-FONC-Gestion de la cryptographie)

**GEC-ADM-05:** Pour l'accès aux interfaces d'administration, le Titulaire doit mettre en place un système d'authentification basé au moins sur deux facteurs ci-dessous, si possible via une solution qualifiée par l'ANSSI ou équivalent:

- Facteur mémoriel- ce qu'il sait (mot de passe, question secrète, etc.)
- Facteur matériel - ce qu'il possède (carte, clé USB, téléphone, etc.)
- Facteur corporel- ce qu'il est (empreinte digitale, réseaux veineux, etc.)
- Facteur -réactionnel - ce qu'il fait (vitesse de frappe, signature, etc.)

**GEC-ADM-06:** Le Titulaire doit utiliser des protocoles et réseau d'administration sécurisés. Il convient de mettre en place un réseau dédié à l'administration des équipements, ou au moins un réseau logiquement séparé de celui des utilisateurs doit être utilisé. Les postes d'administrateurs ou consoles d'administration doivent être dédiés et ne doivent pas pouvoir accéder à Internet.

**Le Titulaire s'engage à respecter l'exigence et à mettre en œuvre les mesures de sécurité décrites ci-dessous: ☐Oui ☐Non**

*Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.*



CNAM / DDSI	Plan Assurance Sécurité	33 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## GEC-COR Gestion des correctifs de sécurité

### Exigence de la Cnam :

Le Titulaire s'engage à mettre en œuvre tous les moyens nécessaires pour garantir la mise en place des correctifs de sécurité nécessaires aux ressources informatiques (postes de travail, serveurs, applications ...) utilisés dans le cadre de la prestation pour éviter toute exploitation des vulnérabilités techniques.

**GEC-COR-01:** Le Titulaire doit mener une veille en matière de vulnérabilité sur l'ensemble des ressources informatiques (postes de travail, serveurs, logiciel ...) utilisés dans le cadre de la prestation.

**GEC-COR-02:** Lorsqu'une vulnérabilité est identifiée, le Titulaire doit notifier à la Cnam les impacts et risques potentiels sur les activités de la prestation et doit déterminer les actions à entreprendre, à savoir:

-Installer un correctif sur les systèmes vulnérables,

-Appliquer d'autres mesures palliatives si les correctifs ne sont pas disponibles.

**GEC-COR-03:** Un suivi périodique de l'état de mise à jour des correctifs de sécurité des composants logiciels et techniques du Titulaire doit être effectué et formalisé. La périodicité sera à définir conjointement avec la Cnam.

**Le Titulaire s'engage à respecter l'exigence et à mettre en œuvre les mesures de sécurité décrites ci-dessous: ☐Oui ☐Non**

*Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.*

CNAM / DDSI	Plan Assurance Sécurité	34 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## GEC-CRYPT Gestion des fonctions cryptographiques

### Exigence de la Cnam :

Le Titulaire s'engage à appliquer les règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de l'ANSSI, version en vigueur [ANSSI-RGS-B1] lorsque qu'il met en place les fonctions cryptographiques, par exemple:

- le chiffrement des données en stockage ;
- le chiffrement des flux ;
- le hachage de mot de passe des utilisateurs et des comptes techniques ;
- la non - répudiation(signature électronique) ;
- l'anonymisation ;
- la génération des aléas

Le Titulaire doit préciser les fonctions cryptographiques mises en œuvre et les mécanismes associés (ex. algorithme, longueur de clés...) pour garantir leur utilisation correcte et efficace.

*[ANSSI-RGS-B1]: Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI, version en vigueur*  
[https://www.ssi.gouv.fr/uploads/2014/11/RGS\\_v-2-0\\_B1.pdf](https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B1.pdf).

**Le Titulaire s'engage à respecter l'exigence et à mettre en œuvre les mesures de sécurité décrites ci-dessous: ☐Oui ☐Non**

*Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.*

CNAM / DDSI	Plan Assurance Sécurité	35 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## GEC-CRYPT-CLE Gestion des clés cryptographiques

### Exigence de la Cnam :

Le Titulaire s'engage à appliquer les règles et recommandations concernant la gestion des clés cryptographiques de l'ANSSI, version en vigueur [ANSSI-CRYPTO-02] lorsque qu'il met en place les fonctions cryptographiques implémentées dans le cadre de la prestation (cf. GEC-CRYPT),

**GEC-CRYPT-CLE-01:** Le Titulaire doit préciser les principes d'architecture de gestion des clés.

**GEC-CRYPT-CLE-02:** Le Titulaire doit préciser comment il protège l'accès aux clés par des moyens à l'état de l'art (ex. conteneur

[ANSSI-RGS-B2]: Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI, version en vigueur  
[https://www.ssi.gouv.fr/uploads/2014/11/RGS\\_v-2-0\\_B2.pdf](https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B2.pdf).

**Le Titulaire s'engage à respecter l'exigence et à mettre en œuvre les mesures de sécurité décrites ci-dessous:** ☐Oui ☐Non

*Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.*

## 5.7 CONTROLE DE L'ACCES ET DES HABILITATIONS (CAH)

### CAH-ACC Gestion de l'accès à des ressources du SI Cnam

### Exigence de la Cnam :

Lors du support et de la maintenance, les accès aux ressources du SI de l'Assurance Maladie doivent être réalisés dans le respect des procédures de gestion des accès Cnam et en conformité avec la politique de sécurité afférente selon la sensibilité des environnements accédés.

Il peut notamment lui être demandé de passer par un matériel de type bastion ou serveur de rebond selon les protocoles autorisés.

**Le Titulaire s'engage à respecter l'exigence:** ☐Oui ☐Non

*Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.*

CNAM / DDSI	Plan Assurance Sécurité	36 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## CAH-GAH Politique de gestion des accès et des habilitations

### Exigence de la Cnam :

Le Titulaire s'engage à de mettre en place une politique de gestion des accès aux données et aux ressources informatiques afin de s'assurer que ceux-ci soient limités aux seules personnes autorisées. La politique de contrôle d'accès et d'habilitation du Titulaire doit respecter à minima les principes de séparation de tâche, de moindre privilège et du besoin d'en connaître.

**CAH-GAH-01:** Le Titulaire doit formaliser une procédure formelle d'enrôlement d'un utilisateur (e.g. exploitant, mainteneur, administrateur ou utilisateur final) d'attribution et de révocation ses droits d'accès sur les données, les ressources informatiques utilisées dans le cadre de la prestation, et de fourniture des moyens d'authentification aux utilisateurs.

**CAH-GAH-02 :** Le titulaire doit respecter le processus d'accès à ODIGO.

**CAH-GAH-03 :** Chaque téléconseiller doit s'engager à verrouiller son PC dès qu'il quitte son poste de travail.

**CAH-GAH-04:** Le Titulaire doit garantir que chacune des personnes devant accéder à des ressources informatiques et/ou réseau de la Cnam dans le cadre de la prestation dispose d'un compte nominatif personnel utilisé uniquement par cette personne tout au cours de la vie du compte.

**CAH-GAH-05:** Le Titulaire doit d'effectuer une revue périodique des droits d'accès aux données et aux ressources informatiques utilisées dans le cadre de la prestation.

**CAH-GAH-06:** Le Titulaire doit tracer les actions d'administration des droits d'accès (requête, validation, attribution, revue et révocation des droits d'accès). Les enregistrements des traces doivent préciser au minimum:

- L'identifiant utilisé pour réaliser les actions d'administration des droits,
- Le type d'action,
- L'horodatage.

**Le Titulaire s'engage à respecter l'exigence et à mettre en œuvre les mesures de sécurité décrites ci-dessous: ☐Oui ☐Non**

*Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.*

CNAM / DDSI	Plan Assurance Sécurité	37 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## CAH-AUT Gestion de l'authentification

### Exigence de la Cnam :

Le Titulaire s'engage à mettre en place les moyens d'identification et d'authentification d'un utilisateur pour identifier sans ambiguïté la personne autorisée à accéder aux données ou aux ressources informatiques utilisés dans le cadre de la prestation (ex. outil télédiagnostic, outil web gestion d'incident) en vue d'empêcher l'usurpation d'identité d'un utilisateur légitime.

**CAH-AUT-01:** Le Titulaire doit formaliser et mettre en œuvre des procédures de gestion de l'authentification des utilisateurs. La gestion des facteurs d'authentification et les sessions doit respecter au minimum les règles à l'état de l'art suivantes:

- L'utilisation des facteurs d'authentification personnels (ex. identifiant et mot de passe),
- Le stockage des codes secrets d'authentification sous forme protégée (ex: mot de passe transformé par une fonction cryptographique irréversible),
- Le transfert des codes secrets d'authentification via des protocoles ou canaux protégés (ex. mise en main propre, chiffrement de flux)
- La robustesse des codes secrets (ex. longueur d'un mot de passe (8 caractères minimum) et sa complexité (alphabétique, numérique et caractères spéciaux))
- Le renouvellement périodique des codes secrets (ex. 90 jours),
- Le verrouillage de session suite à la détection d'inactivité d'un utilisateur authentifié. Le déverrouillage doit nécessiter l'utilisation des facteurs d'authentification (ex. identification et code secret).

**CAH-AUT-02:** Le Titulaire doit tracer les actions des administrateurs des comptes, les accès ou tentatives de connexion des utilisateurs. Les enregistrements des traces doivent préciser au minimum:

- L'identifiant utilisé pour réaliser les actions d'administration, les connexions ou tentatives de connexions,
- Le type d'action,
- L'horodatage.

**Le Titulaire s'engage à respecter l'exigence et à mettre en œuvre les mesures de sécurité décrites ci-dessous: ☐Oui ☐Non**

*Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.*

CNAM / DDSI	Plan Assurance Sécurité	38 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## CAH-TRA Gestion de la traçabilité

### Exigence de la Cnam :

Les traces d'accès ou d'usage de ressources de la Cnam enregistrées par le Titulaire dans le cadre de la prestation doivent être imputables à un individu et horodatées selon une référence horaire commune à l'ensemble des équipements d'un même réseau.

**CAH-TRAC-01:** Le prestataire doit documenter et mettre en œuvre une politique de journalisation dans le cadre de la prestation. En particulier, le Titulaire doit tracer tout accès sur le SI et les données de l'Assurance Maladie et consigner les interventions. Il est également tenu d'être en mesure d'identifier toute personne ayant accédé au SI depuis ses systèmes. Les éléments de journalisation nécessaires à cette identification doivent être protégés contre toute modification.

Le Titulaire est tenu de mettre à disposition de la Cnam les informations journalisées si nécessaire.

D'autre part, le Titulaire est tenu de conserver ces traces au minimum [A compléter: la durée XXX (par défaut à minima 6 mois)].

**CAH-TRAC-02:** Le Titulaire est tenu de ne pas désactiver les mécanismes de traçabilité mis en œuvre dans le cadre de la prestation. La Cnam pourra ponctuellement demander une consultation des traces générées et stockées dans le cadre de la prestation du Titulaire.

**CAH-TRAC-03:** Le Titulaire doit réaliser une revue et analyse périodique des journaux et événements de sécurité afin de détecter les erreurs, dysfonctionnements, tentatives d'accès illicites, et violation des règles de sécurité applicables à la prestation.

**Le Titulaire s'engage à respecter l'exigence et à mettre en œuvre les mesures de sécurité décrites ci-dessous: ☐Oui ☐Non**

*Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.*

CNAM / DDSI	Plan Assurance Sécurité	39 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## 5.8 SECURITE DU SUPPORT ET DE MAINTENANCE (SUP)

### SUP-DONNEES

### Protection des données

#### Exigence de la Cnam :

Le Titulaire s'engage à mettre en place un cloisonnement entre les flux suivants:

- Supervision qui consiste à remonter les informations (traces, dump, données de configuration) vers le Titulaire pour le diagnostic, la surveillance de fonctionnement, la gestion des incidents
- Maintenance qui consiste à exécuter des commandes (ex. restauration, redémarrage, reset...) et mettre à jour des micro-logiciels embarqués (ex. firmware) modifiant le fonctionnement d'un équipement et/ou logiciel

**Par défaut, le Titulaire doit réaliser la maintenance « sur site » dans les locaux et sous la surveillance d'un agent de la Cnam et le télédiagnostic. Dans le cas où les actions de télémaintenance se présentent au cours du marché, il est nécessaire de mettre en place une procédure d'exception respectant au minimum les conditions de sécurité spécifiques stipulées par les exigences SUP-OPER et SUP-SUIV. La Cnam se réserve le droit de refuser la maintenance « hors site » ou d'ajouter d'autres exigences selon le contexte et l'environnement de l'équipement objet de maintenance à distance.**

**SUP-DONNEES-01:** Les composants de l'outil télédiagnostic(ex. agent et console de visualisation)n'utiliseront que les informations techniques strictement nécessaires à l'analyse et la supervision de fonctionnement des matériels et logiciels associés. Le Titulaire précise les informations et les données auxquelles l'outil de télédiagnostic accède pour la supervision de fonctionnement des matériels et logiciel associés (ex. remontée de l'information concernant le numéro de série, version, indicateur de fonctionnement, indicateur de consommation CPU, etc.)

**SUP-DONNEES-02:** Le mainteneur et l'outil de maintenance n'accéderont qu'aux informations techniques des matériels et logiciels associés nécessaires à leur maintien en conditions opérationnels. Le Titulaire précise les informations et les données accédées par le personnel et par l'outil de maintenance.

**SUP-DONNEES-03:** Le Titulaire s'interdit d'exploiter de manière frauduleuse les données Métier sensibles contenues éventuellement dans les traces et dump(ex. données à caractère personnel, données médicales) lors de la résolution et/ou reproduction d'un incident. Ces traces et dump doivent être supprimées conformément aux modalités définis par l'exigence **GEC-DON-04**.

**Le Titulaire s'engage à respecter l'exigence et à mettre en œuvre les mesures de sécurité décrites ci-dessous: ☐Oui ☐Non**

*Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.*

CNAM / DDSI	Plan Assurance Sécurité	40 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## SUP-OPER

## Opération de support et maintenance à distance

### Exigence de la Cnam :

Les opérations de support et de maintenance « hors site » via un accès à distance ne doivent pas être possibles sans autorisation de la Cnam et en dehors des périodes de maintenance.

**SUP-OPER-01:** Le Titulaire doit établir conjointement avec la Cnam:

- La liste exhaustive des systèmes accédés ;
- La liste du personnel effectuant les actes de support et de maintenance ;
- La liste des services et opérations à réaliser sur chaque système ;
- La liste des comptes d'accès et des droits associés. Il est nécessaire de mettre en place des comptes d'accès dédiés au Titulaire avec les droits limités en respectant le principe de moindre privilège et le besoin d'en connaître (cf. Exigence CAH-GAH).
- Les plages horaires d'intervention.

Ces listes devront être tenues à jour pendant toute la durée de la prestation. Toute évolution nécessitera une validation formelle par la Cnam.

**SUP-OPER-02:** Le Titulaire doit privilégier les accès temporaires aux accès permanents. Chaque connexion à distance devra fait l'objet de demande, de validation et contrôle par le RSSI Cnam (ou son délégué) du site hébergeant l'équipement ou logiciel à maintenir.

**SUP-OPER-03:** Le Titulaire devra formaliser la procédure d'intervention à distance en détaillant modalités d'intervention à distance (cf. SUP-OPER-01) et le circuit de demande, de validation, et le contrôle des accès et connexions (cf. SUP-OPER-02).

**SUP-OPER-04:** Le Titulaire devra formaliser le dossier d'architecture sécurité de l'outil de télémaintenance, qui sera soumis à la validation formelle d'une instance de Sécurité de la Cnam (ex. RSSI du site) avant sa mise en service. Ce dossier d'architecture détaillera à minima les informations ci-dessous:

- Le contrôle d'accès des utilisateurs et des habilitations associées.
- La matrice de flux avec la spécification technico – fonctionnelle de chaque flux.
- La gestion de trace.

**Le Titulaire s'engage à respecter l'exigence ci-dessous: ☐Oui ☐Non**

*Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.*



CNAM / DDSI	Plan Assurance Sécurité	41 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## SUP-SUIVI

## Suivi et contrôle des actions en temps réel

### Exigence de la Cnam :

Dans le cas d'actes de support et maintenance réalisés à distance, le Titulaire s'engage à mettre en place un outil de télémaintenance permettant à la Cnam de contrôler et suivre les actions réalisées en temps réel. L'outil de télémaintenance doit être capable d'implémenter à minima les principes directeurs suivants:

- Permettre à la Cnam de contrôler et participer activement à toutes les sessions de prise de main à distance
- Permettre à la Cnam de suivre et voir toutes les actions d'une session ouverte en temps réels par exemple quelle donnée visualisée, quelle commande exécutée, quelle navigation entreprise.
- Permettre à la Cnam d'interrompre une session ouverte à tout moment et n'importe quel motif.

**Le Titulaire s'engage à respecter l'exigence: ☐Oui ☐Non**

*Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.*

## SUP-ACTION

## Transparence des actions

### Exigence de la Cnam :

Le Titulaire est tenu de garantir la transparence de ces actions. Les outils de support et de maintenance déployés doivent offrir la possibilité au personnel de la Cnam de vérifier les actions réalisées dans le cadre d'actes de support et maintenance. Les commandes effectuées doivent pouvoir être tracées et un fichier de traces doit être disponible sur le système maintenu.

La Cnam attend du Titulaire qu'il décrive les outils utilisés, protocoles d'accès, ainsi qu'un schéma d'architecture technique.

**Le Titulaire s'engage à respecter l'exigence et à mettre en œuvre les mesures de sécurité décrites ci-dessous: ☐Oui ☐Non**

*Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.*

CNAM / DDSI	Plan Assurance Sécurité	42 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## SUP-DURC

## Durcissement de configuration

### Exigence de la Cnam :

Afin prémunir la Cnam contre les failles de sécurité, le Titulaire est tenu de mettre à disposition de la Cnam des guides de bonnes pratiques de sécurité et/ou des recommandations de configuration sécurisée des équipements ou matériels ou logiciel dans le cadre de la prestation Support et/ou Assistance Technique du marché.

**Le Titulaire s'engage à respecter l'exigence: ☐Oui ☐Non**

*Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.*

CNAM / DDSI	Plan Assurance Sécurité	43 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## 5.9 GESTION DES INCIDENTS (GDI)

GDI-INC	Traitement des incidents de sécurité
	<p><b>Exigence de la Cnam :</b></p> <p>Le Titulaire s'engage à disposer, sur le périmètre de la prestation, d'un processus formalisé et opérationnel de gestion des incidents de sécurité. Celui devra tenir compte des phases suivantes:</p> <ul style="list-style-type: none"> <li>- détection,</li> <li>- analyse,</li> <li>- alerte à la Cnam,</li> <li>- traitement.</li> </ul> <p>Le Titulaire doit permettre à Cnam de participer au traitement de l'incident le cas échéant.</p> <p><b>GEC-INC-01:</b> Le processus de gestion d'incident doit décrire à minima:</p> <ul style="list-style-type: none"> <li>- les intervenants, rôles, responsabilités et coordonnées</li> <li>- les Modes opératoires de qualification, alerte, traitement et clôture des incidents de sécurité</li> <li>- la matrice de qualification des incidents de sécurité</li> <li>- les modalités d'analyse post-incident avec la Cnam afin de traiter les causes approfondies, et établir le plan d'amélioration continue.</li> </ul> <p>Le processus de gestion d'incidents de sécurité doit être fait l'objet de revue et de validation de manière conjointe par les parties prenantes Titulaire et la Cnam.</p> <p><b>GEC-INC-02:</b> Le Titulaire est tenu de garantir la non-diffusion des informations sur les incidents de sécurité et leur documentation afin d'éviter que des vulnérabilités sur des logiciels cœur de métier ne soient rendues accessibles ou publiques.</p> <p><b>GEC-INC-03:</b> Le Titulaire s'engage à notifier à la Cnam (ex. prescripteur du marché, DPO) toute violation de données à caractère personnel relevant du périmètre de la prestation sans délais après en avoir pris connaissance conformément au RGPD en vigueur(cf. Article 33 du RGPD).</p>
	<p><b>Le Titulaire s'engage à respecter l'exigence et à mettre en œuvre les mesures de sécurité décrites ci-dessous: <input type="checkbox"/>Oui <input type="checkbox"/>Non</b></p>
	<p><i>Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.</i></p>

CNAM / DDSI	Plan Assurance Sécurité	44 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## 5.10 GESTION DES TIERS (GDT)

GDT-STR	Sous-traitance
<p><b>Exigence de la Cnam :</b></p> <p>Le Titulaire s'engage, pour l'ensemble des informations manipulées et services mis en œuvre dans le cadre de la prestation, à spécifier précisément à la Cnam les opérateurs (sociétés et fournisseurs) amenés à intervenir en cotraitance et sous-traitance.</p> <p><b>GDT-STR-01:</b> Le Titulaire doit répercuter les clauses du présent PAS dans ses contrats de sous-traitance et de cotraitance et s'assurer de leur mise en œuvre effective. A la demande de la Cnam, le Titulaire doit être capable de présenter les preuves suffisantes quant à la mise en œuvre des exigences du PAS par ses sous –traitants ou cotraitant.</p> <p><b>GDT-STR-02:</b> Dans le cas où le Titulaire recrute un autre sous-traitant ou cotraitance après la signature du contrat, le Titulaire doit obtenir l'autorisation écrite de la Cnam conformément à l'article 28.2 du RGPD en vigueur.</p> <p><i><b>Remarque:</b> La Cnam se réserve le droit de refuser les actes de sous-traitance ou cotraitance de parties essentielles de dit marché aux entreprises dont il n'a pas pu vérifier les capacités techniques et économiques en termes de sécurité. L'ensemble des clauses et engagements de couverture de risques reste à la charge du Titulaire, qui devra se réassurer auprès de son sous-traitant et/ou cotraitant.</i></p>	
<p><b>Le Titulaire s'engage à respecter l'exigence: <input type="checkbox"/>Oui <input type="checkbox"/>Non</b></p>	
<p><i>Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.</i></p>	

CNAM / DDSI	Plan Assurance Sécurité	45 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## 5.11 CONTROLE ET CONFORMITE (CTL)

CTL-AUD	Audit
<p><b>Exigence de la Cnam :</b></p> <p>Le Titulaire s'engage à autoriser la Cnam à réaliser les audits de sécurité le concernant afin de contrôler la bonne mise en œuvre des mesures décrites dans le PAS.</p> <p><b>CTL-AUD-01:</b> Dans ce cadre, le Titulaire doit mettre à la disposition de la Cnam tous les éléments nécessaires à la réalisation de ces audits. Les modalités de réalisation de l'audit de sécurité seront à établir conjointement avec la Cnam:</p> <ul style="list-style-type: none"> <li>-Les mesures de notification préalable (délai, communication du programme d'audit) ;</li> <li>- Les délais de réalisation ;</li> <li>- Les périmètres non auditables, s'il y a lieu ;</li> <li>-La disponibilité des ressources et documentations du Titulaire pour la bonne conduite de l'audit ;</li> <li>- Les engagements en matière de prise en compte des recommandations émises à l'issue d'un audit.</li> </ul> <p><i>Remarque: La Cnam se réserve le droit de déléguer à un tiers la réalisation des audits.</i></p> <p><b>CTL-AUD-02:</b> Le Titulaire est tenu de respecter les exigences du CCTP ainsi que les mesures de sécurité décrites dans le PAS, en cas de contrôle ou d'audit par ses autres clients. Il doit maintenir le niveau de sécurité de la prestation pendant les phases de contrôles et d'audits.</p>	
<p><b>Le Titulaire s'engage à respecter l'exigence et à mettre en œuvre les mesures de sécurité décrites ci-dessous: <input type="checkbox"/>Oui <input type="checkbox"/>Non</b></p>	
<p><i>Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.</i></p>	

CNAM / DDSI	Plan Assurance Sécurité	46 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

#### CTL-CFT Conformité au CCTP et au PAS

##### Exigence de la Cnam :

Le Titulaire s'engage à effectuer l'auto-évaluation de conformité aux exigences de sécurité du présent PAS et celles du CCTP pour garantir le niveau de sécurité au démarrage de la prestation ainsi que son maintien tout au long de la prestation.

**CTL-CFT-01:** De manière transparence, le Titulaire doit fournir et présenter périodiquement le tableau de bord des indicateurs sécurité et le résultat de l'auto-évaluation lors du COPIL du marché. Par défaut, il conviendra d'effectuer à minima l'auto-évaluation annuelle toutefois cette périodicité pourra être revue et établie conjointement avec la Cnam lors du démarrage du marché selon la criticité et la stabilité des prestations.

**CTL-CFT-02:** En cas de constatation d'écarts avec les engagements sur les exigences de sécurité stipulées par la Cnam (PAS et/ou CCTP), des actions correctives devront être réalisées dans un délai convenu d'un commun accord entre la Cnam et le Titulaire.

**Le Titulaire s'engage à respecter l'exigence:** ☐Oui ☐Non

*Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.*

## 5.12 CONFORMITE (CFT)

#### CFT-GEO Lieu géographique de traitement des données

##### Exigence de la Cnam :

**CFT-GEO-01:** Le Titulaire est tenu d'indiquer à la Cnam la liste des différents lieux géographiques de traitement des données dans le cadre de l'exécution des prestations (lieux depuis lesquels les données sont consultées, modifiées, stockées, détruites), notamment quand ces lieux sont situés hors de France.

**CFT-GEO-02:** En cas de modification de la liste des pays où les données sont traitées, le Titulaire devra en informer préalablement la Cnam sans délai et obtenir son autorisation écrite.

**CFT-GEO-03:** Le Titulaire s'engage à effectuer toutes les activités liées à la mise au rebut et au recyclage des matériels d'infrastructure de la Cnam au sein de l'Union Européenne et conformément aux règles définies par la CNIL pour les interventions réalisées hors Union Européenne.

**Le Titulaire s'engage à respecter l'exigence:** ☐Oui ☐Non

*Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.*

CNAM / DDSI	Plan Assurance Sécurité	47 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

### 5.13 PHASE DE REVERSIBILITE (REV)

REV-REV	Restitution du matériel, des données et des codes source
<p><b>Exigence de la Cnam :</b></p> <p>Le Titulaire s'engage à mettre en œuvre des processus de réversibilité en matière de sécurité à la fin de marché pour éviter les fuites d'information ou accès illicites aux données ou au SI de la Cnam.</p> <p><b>REV-SEC-01:</b> le Titulaire doit disposer d'une procédure permettant la restitution et la destruction définitive des données (ou matériels) de la Cnam. Cette procédure décrit notamment:</p> <ul style="list-style-type: none"> <li>• La destruction des données présentes sur tous les environnements (production, qualification, développement)</li> <li>• La destruction des données présentes sur des supports de sauvegardes, même si ceux-ci sont mutualisés.</li> </ul> <p><b>REV-SEC-02:</b> Le Titulaire doit fournir un rapport de destruction qui mentionne au minimum:</p> <ul style="list-style-type: none"> <li>• Le succès ou l'échec de l'opération</li> <li>• Les algorithmes ou la méthode utilisée pour la destruction</li> </ul> <p><b>REV-SEC-03:</b> le Titulaire doit effectuer la révocation de l'ensemble des accès au SI de la Cnam et la fermeture des flux associés.</p>	
<p><b>Le Titulaire s'engage à respecter l'exigence:</b> <input type="checkbox"/>Oui <input type="checkbox"/>Non</p>	
<p><i>Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.</i></p>	

REV-MCOS	Maintien du niveau de sécurité durant la réversibilité ou transfert de prestation
<p><b>Exigence de la Cnam :</b></p> <p>En cas d'arrêt de la prestation (fin de contrat ou activation de la clause de réversibilité par exemple), le Titulaire s'engage à assurer le maintien du niveau de sécurité de la prestation décrit dans ce présent PAS pendant toute la phase de transfert de prestations vers son successeur.</p> <p><b>REV-MCOS-01:</b> A la demande de la Cnam, le Titulaire doit mettre en place un canal de communication sécurisée, de manière temporaire, permettant le transfert des données vers son successeur. Ce canal de transfert peut s'appuyer typiquement sur la technologie VPN IPSEC.</p> <p><b>REV-MCOS-02:</b> Pour le respect de besoins légaux, les exigences du présent PAS liées à la conservation des traces sont toujours applicables après l'arrêt de la prestation.</p>	
<p><b>Le Titulaire s'engage à respecter l'exigence:</b> <input type="checkbox"/>Oui <input type="checkbox"/>Non</p>	
<p><i>Le Titulaire décrit ici les moyens qu'il s'engage à mettre en œuvre pour le respect de l'exigence formulée par la Cnam.</i></p>	

CNAM / DDSI	Plan Assurance Sécurité	48 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

## 6. EXEMPLES D'INDICATEURS

Ce chapitre liste les indicateurs type permettant le suivi de la SSI de la prestation. Le choix des indicateurs dépendra du contexte du marché et des principaux risques à couvrir. Le Titulaire proposera les valeurs cibles de chaque indicateur retenu. Le Titulaire et la Cnam peuvent définir conjointement d'autres indicateurs en fonction du besoin.

Chapitre	Indicateur
ORG	Nombre de perte et/ou de vol de documents (papier ou électronique).
	Date de la dernière revue de sécurité dans un comité de gouvernance.
CLA	Nombre de mise à jour de l'inventaire des moyens sensibles (ou documents sensibles)
DIS	Fréquence des exercices de crise (mise en œuvre du PCA ou PRA).
	Taux de disponibilité du service externalisé.
SRH	Taux de renouvellement de formation par an.
	Taux de personnel ayant reçu une formation sécurité, en lien avec les métiers exercés.
	Taux de personnel ayant suivi une sensibilisation à la sécurité.
	Taux d'engagement individuel de confidentialité signé.
SPH	Périodicité de mise à jour de la liste des accès physiques.
	Nombre de déclaration de perte de badge sur l'année.
	Nombre d'incidents de sécurité physique détectés sur l'année (intrusion, vol de matériel, perte de matériel, ...).
	Nombre d'incidents de sécurité physiques sur des actifs sensibles (vol ou perte de documents ou matériel, mise au rebut non sécurisée, ...).
	Nombre de maintenance/an des équipements de sécurité physiques (détecteur d'intrusion, alarme d'incendie, climatisation, etc.)
	Taux de postes de travail (fixes / portables) dont le disque dur est chiffré.
	Proportion de postes de travail (fixes / portables) sécurisés par un câble antivol.
GEC	Taux de sauvegarde réalisée (à partir de la périodicité définie).
	Taux d'analyse des journaux de sécurité (à partir de la périodicité définie).
	Taux de systèmes (serveurs et postes de travail) à jour au niveau de: <ul style="list-style-type: none"> <li>• Correctifs de sécurité ;</li> <li>• Signature -antivirus ...</li> </ul>
	Nombre de maintenances réalisées sur site.
	Durée d'indisponibilité du SI/selon les exigences contractuelles.
CAH	Périodicité de mise à jour de la liste des accès logiques.
	Périodicité de revue d'habilitation et de comptes d'accès.
	Taux d'anomalie de comptes d'accès (ex: compte orphelin, conflit de droits d'accès, etc.)
GDI	Taux d'incident lié à la non-application des procédures.
	Nombre d'incidents de sécurité SI sur <une période à définir>.
	Taux augmentation ou diminution des incidents.
GDT	Dans le cadre de la prestation, taux de sous-traitance visés par le service juridique et la direction de sécurité (cf. démarche de PAS ou équivalente).
CTL	Nombre de revues de configuration réalisés par an.
	Nombre d'audits réalisés sur un an par le Titulaire.



CNAM / DDSI	Plan Assurance Sécurité	49 / 49
Direction Sécurité	Maintenance et Support des infrastructures	Date : 16/10/2024

**Fin du document**