

Maîtriser

## Sécurité des Systèmes d'Information

Règles de sécurité du Système d'Information  
applicables aux titulaires de marché de l'AP-HP

Octobre 2018 – Version 1.3 – Diffusion Publique

# Règles de sécurité du Système d'Information applicables aux titulaires de marché de l'AP-HP

Classification	Diffusion Publique	
Fichier	14DI-CharteTitulaireMarché-20181001V13.docx	
Version	1.3	
Etat du document	Validé	
Date	01/10/2018	
PJ	N/A	
Suivi des mises à jour		
Version	Date de mise à jour	Motif
1.3	01/10/2018	Suppression de la possibilité d’avoir une télémaintenance non nominative Mise à jour du formulaire
1.2	23/02/2017	Intégration des observations de la société TEAMNET Intégration des observations du DSIP sur le chiffrement et l’indisponibilité de la télémaintenance.
1.1	08/11/2016	Intégration des observations du CCSP et de la DAJ
1.0	03/03/2016	Validation.
0.5	21/01/2016	Prise en compte des observations d’ACHAT
0.1	17/11/2015	Création du document

## TABLE DES MATIERES

<b>1</b>	<b>PREAMBULE</b>	<b>4</b>
1.1	Définitions	4
1.2	Objectifs	4
1.3	Portée et effet	5
<b>2</b>	<b>PROTECTION ET CONFIDENTIALITE DES INFORMATIONS</b>	<b>5</b>
2.1	Cas particulier d'accès aux données nominatives de santé	7
<b>3</b>	<b>ACCES PHYSIQUES</b>	<b>7</b>
3.1	Accès physiques aux locaux	7
3.2	Vidéoprotection	8

3.3	Connexion du matériel du TITULAIRE DE MARCHÉ sur le réseau .....	9
<b>4</b>	<b>ACCES LOGIQUES .....</b>	<b>9</b>
4.1	Généralités .....	9
4.2	Sécurité des accès logiques .....	10
4.3	Protection contre les logiciels malveillants .....	11
<b>5</b>	<b>TELEMAINTENANCE .....</b>	<b>11</b>
5.1	Généralités .....	11
5.2	Connexion depuis l'extérieur .....	11
<b>6</b>	<b>SPECIFICITE DANS LES INTERVENTIONS.....</b>	<b>13</b>
6.1	Généralités .....	13
6.2	Engagements du TITULAIRE DE MARCHÉ .....	13
6.3	Incidents .....	13
<b>7</b>	<b>PRESTATIONS ET MAINTIEN EN CONDITION DE SECURITE .....</b>	<b>14</b>
7.1	Informations quant aux risques.....	14
7.2	Homologation de sécurité .....	14
7.3	Téléservices de l'administration électronique .....	14
7.4	Mises à jour .....	14
7.5	Gestion des vulnérabilités techniques .....	15
<b>8</b>	<b>AUDITS.....</b>	<b>16</b>
8.1	Audit par le TITULAIRE DE MARCHÉ.....	16
8.2	Audit par l'AP-HP.....	17
<b>9</b>	<b>TRACABILITE .....</b>	<b>18</b>
9.1	Traçabilité des accès pour les comptes génériques.....	18
<b>10</b>	<b>ASPECTS JURIDIQUES .....</b>	<b>18</b>
10.1	Responsabilité .....	18
10.2	Respect des lois en vigueur .....	19
10.3	Intitulé des clauses .....	19
10.4	Invalidité d'une clause .....	19
10.5	Exceptions .....	19

## 1 PREAMBULE

---

### 1.1 Définitions

**« DSI »**

Direction des Systèmes d'Informations.

**« TITULAIRE DE MARCHÉ »**

FOURNISSEUR du marché auquel est annexée la présente charte, ainsi que ses éventuels sous-traitants dont il fait son affaire et pour lesquels il s'engage.

**« Marché »**

Contrat de prestations de services, de fournitures de matériels ou de logiciels / progiciels, de travaux, etc., liant contractuellement au sens du Code des Marchés Publics un FOURNISSEUR à l'AP-HP. La présente charte est annexée au marché.

**« RSSI »**

Responsable Sécurité des Systèmes d'Information.

**« Système d'information (SI) »**

On entend par Système d'Information (ci-après le « SI ») l'ensemble des ressources - matérielles et logicielles - des moyens techniques, des procédures et moyens humains et organisationnels, mis en jeu dans la création, le stockage, le traitement, l'archivage, la transmission, la diffusion et la communication des données et informations utilisées dans le fonctionnement de l'entreprise. Cela inclut entre autres : les logiciels (applications informatiques, systèmes de messagerie électronique, outils bureautiques, systèmes d'exploitation, outils d'administration, utilitaires, bases de données...), les matériels informatiques ou bureautiques (serveurs, ordinateurs et téléphones – fixes ou portables –, PDA, imprimantes et photocopieurs, etc.), les équipements des réseaux de données (routeurs, commutateurs, autocommutateurs, fax...), les médias de stockage (disques durs, CD-ROM, clés USB, ...) et les équipements de production.

### 1.2 Objectifs

La présente charte s'inscrit dans une démarche d'information, de sensibilisation et de responsabilisation des TITULAIRES DE MARCHÉ afin de poser les règles d'accès et d'utilisation des Systèmes d'Information (SI) de l'AP-HP.

Elle a pour objet de définir les conditions et modalités, que le TITULAIRE DE MARCHÉ s'engage à respecter, afin d'assurer la sécurité des SI de l'AP-HP ainsi que de ses données. L'objectif consiste ainsi à éviter que les relations avec les TITULAIRES DE MARCHÉ ne constituent une faille dans les règles de sécurité informatique définies par la Politique Générale de Sécurité du Système d'Information de l'AP-HP.

# Règles de sécurité du Système d'Information applicables aux titulaires de marché de l'AP-HP

Le TITULAIRE DE MARCHÉ est soumis à une obligation d'information, de conseil et de mise en garde auprès de l'AP-HP, incluant l'appréhension des risques de sécurité de l'information induits par la mise en œuvre de ses prestations.

Cette charte et les règles qu'elle contient ont été établies en tenant compte de la Politique de Sécurité de l'AP-HP et sous l'autorité du Responsable de la Sécurité des Systèmes d'Information. Elle fait partie du référentiel de sécurité de l'AP-HP approuvé par la Direction Générale de l'établissement. Elle complète tout Marché liant le TITULAIRE DE MARCHÉ à l'AP-HP. Son respect constitue une obligation essentielle à la charge du TITULAIRE DE MARCHÉ.

## 1.3 Portée et effet

Cette charte s'applique à tous les TITULAIRES DE MARCHÉ, quel que soit le support juridique (marché, simple facture...), qui doit avoir accès à tout ou partie du Système d'Information de l'AP-HP. Le TITULAIRE DE MARCHÉ doit se conformer à ses dispositions.

La présente charte s'applique au TITULAIRE DE MARCHÉ et à ses préposés. Elle s'applique également à tout opérateur économique intervenant pour le compte ou en partenariat avec le TITULAIRE DE MARCHÉ (cotraitants et sous-traitants notamment).

Pour les marchés informatiques, la présente charte constitue une des pièces du marché. Pour les autres marchés, elle est annexée au Cahier des Clauses Administratives Particulières.

Elle s'applique à compter de la date de publication mentionnée sur la page de garde de ce document.

Ses dispositions sont applicables dès la notification du marché au quel elle est annexée. Elles restent en vigueur pour toute la durée du marché.

Comme tout utilisateur du Système d'Information de l'AP-HP, tout préposé du TITULAIRE DE MARCHÉ est soumis à la Charte Utilisateur du Système d'Information annexée au règlement intérieur de l'AP-HP. La présente Charte TITULAIRE DE MARCHÉ décrit les dispositions additionnelles spécifiques applicables au TITULAIRE DE MARCHÉ vis-à-vis du Système d'Information de l'AP-HP.

Sauf mention contraire, le TITULAIRE DE MARCHÉ est soumis à une obligation de moyen, étant entendu que la charge de la preuve lui incombe.

## 2 PROTECTION ET CONFIDENTIALITE DES INFORMATIONS

---

Toute donnée dont le TITULAIRE DE MARCHÉ a connaissance à l'occasion de l'exécution du marché est strictement couverte par le secret professionnel en application de l'article 226-13 du Code pénal. Ne constituent pas des informations confidentielles les informations qui :

- (i) Sont déjà connues du TITULAIRE DE MARCHÉ qui les reçoit préalablement à la date de leur divulgation par l'AP-HP.

## Règles de sécurité du Système d'Information applicables aux titulaires de marché de l'AP-HP

- (ii) Sont disponibles dans le domaine public lors de leur divulgation ou tombent ultérieurement dans le domaine public, sans manquement aux stipulations du marché.
- (iii) Sont communiquées par un tiers à titre non confidentiel au TITULAIRE DE MARCHÉ, dès lors que ce tiers n'est pas lié à l'autre partie par une quelconque obligation de confidentialité.
- (iv) Sont développées de manière indépendante par le FOUNISSEUR qui les reçoit, en dehors de tout manquement aux stipulations au marché.

Le TITULAIRE DE MARCHÉ veille à ce qu'au cours de l'exécution du présent marché, soient respectées la sécurité et la confidentialité des données et des accès informatiques de l'AP-HP conformément aux lois et régimes applicables, et notamment conformément à la loi n° 78-17 du 6 janvier 1978 modifiée par la Loi du 6 août 2004 relative à l'informatique, aux fichiers et aux libertés, et aux dispositions du Code pénal en vigueur.

A ce titre, le TITULAIRE DE MARCHÉ s'engage à :

1. N'utiliser les informations et documents délivrées par l'AP-HP que pour la finalité définie dans le marché
2. Ne pas divulguer à des tiers, à titre gratuit ou onéreux, et sous quelque forme que ce soit, les informations et documents communiqués par l'AP-HP à l'occasion de l'exécution du marché
3. Prendre toutes les mesures pour que lesdites données ne puissent être accessibles à d'autres personnes que les personnels attachés à leur traitement et à leur analyse. Ces derniers seront sensibilisés au caractère stratégique des informations et documents confiés et liés au TITULAIRE DE MARCHÉ par un engagement de confidentialité
4. Ne pas procéder à des copies, utilisations ou diffusion de partie ou totalité d'un fichier et/ou d'une donnée détenue par l'AP-HP à l'exception des copies, utilisations ou diffusion nécessaires à l'exécution d'une prestation prévue au marché, auquel cas l'accord de l'AP-HP est nécessaire
5. Ne pas sortir des locaux de l'AP-HP des configurations, des supports numériques ou d'autres, d'éléments ou sous-ensembles d'une configuration, d'un matériel, ou d'une documentation détenue par l'AP-HP sans l'autorisation préalable et écrite de celle-ci
6. Informer l'AP-HP de toute réception par lui d'une mise en demeure, réquisition ou requête judiciaire, de toute enquête ou toute autre notification relative à la réalisation des prestations
7. Chiffrer les informations présentes sur ses équipements utilisés ou transportés hors de ses locaux, comportant des informations nominatives, avec un logiciel de chiffrement ayant fait l'objet d'une certification CSPN par l'ANSSI (<http://www.ssi.gouv.fr/fr/certificationqualification/cspn/>).

Le TITULAIRE DE MARCHÉ est responsable vis-à-vis de l'AP-HP de la perte de documents remis sous quelque forme que ce soit, ou de la divulgation volontaire ou involontaire d'informations communiquées. Le TITULAIRE DE MARCHÉ s'engage, à ce titre, à aviser sans délai l'AP-HP de toute disparition, ainsi que de tout incident pouvant révéler un risque de violation des présentes obligations.

Le TITULAIRE DE MARCHÉ procède à la destruction ou à la restitution de tous les fichiers manuels ou informatisés stockant les informations saisies, à l'échéance du présent marché, sur ordre de l'AP-HP.

Ces dispositions s'appliquant au TITULAIRE DE MARCHÉ mais également à tout opérateur économique intervenant pour le compte ou en partenariat avec le TITULAIRE DE MARCHÉ (cotraitants et sous-traitants notamment).

## Règles de sécurité du Système d'Information applicables aux titulaires de marché de l'AP-HP

L'AP-HP se réserve le droit de procéder à toute vérification, notamment par des audits (cf. Audit par l'AP-HP à la page n°17 et suivante) qui lui paraîtrait nécessaire pour constater le respect des obligations de confidentialité par le TITULAIRE DE MARCHÉ.

En cas de non-respect des dispositions précitées, la responsabilité du TITULAIRE DE MARCHÉ peut également être engagée sur la base des dispositions des articles 226-5 et 226-17 du code pénal.

L'AP-HP se réserve le droit d'exiger du TITULAIRE DE MARCHÉ du marché, sans versement d'aucune indemnité, le remplacement immédiat de tout agent salarié de l'entreprise qui aurait contrevenu aux règles précédemment édictées.

L'AP-HP peut prononcer la résiliation immédiate du marché, sans indemnité en faveur du TITULAIRE DE MARCHÉ, en cas de violation du secret professionnel ou de non-respect des dispositions précitées.

### 2.1 Cas particulier d'accès aux données nominatives de santé

Au cas où le TITULAIRE DE MARCHÉ serait en position d'accéder à des données nominatives de santé, il est rappelé que les dispositions juridiques en vigueur imposent pour l'accès à ces données d'un moyen d'authentification forte validé par l'ASIP Santé (Cf. : PGSSI-S : Politique générale de sécurité des systèmes d'information de santé - Référentiel d'authentification des acteurs de santé).

En particulier, le TITULAIRE DE MARCHÉ devra porter un soin particulier à l'accès à ces données nominatives de santé lors d'opérations de télémaintenance. Le TITULAIRE DE MARCHÉ devra prendre toutes les dispositions nécessaires pour qu'en aucun cas les données nominatives de santé ne sortent de l'AP-HP.

## 3 ACCES PHYSIQUES

---

### 3.1 Accès physiques aux locaux

L'AP-HP assure au personnel du TITULAIRE DE MARCHÉ appelé à intervenir dans ses locaux, des conditions d'environnement conformes aux normes d'hygiène et de sécurité. L'AP-HP doit informer le TITULAIRE DE MARCHÉ des consignes de sécurité dans lesdits locaux, et veiller à la présence effective de l'un de ses préposés qualifiés pendant la durée de l'intervention dudit personnel, de telle sorte que toutes mesures utiles puissent être immédiatement prises en cas d'accident.

L'accès aux locaux de l'AP-HP par le TITULAIRE DE MARCHÉ est soumis aux règlements intérieurs imposés aux personnes extérieures à l'AP-HP. L'AP-HP s'engage à limiter l'accès à l'ensemble de ses installations informatiques et télécoms et à mettre en place une procédure interne permettant de s'assurer qu'aucune personne étrangère au service et non autorisée ne peut accéder au local où sont hébergées les informations traitées dans le cadre du présent marché.

## Règles de sécurité du Système d'Information applicables aux titulaires de marché de l'AP-HP

Les locaux où le TITULAIRE DE MARCHÉ est hébergé ainsi que les moyens d'accès physiques lui sont communiqués par l'AP-HP. Le TITULAIRE DE MARCHÉ s'engage à suivre les règles suivantes :

- Ne pas essayer de s'introduire dans des salles non autorisées ou avec d'autres moyens que ceux mis à sa disposition
- Ne pas permettre l'accès aux personnes non autorisées par l'AP-HP dans les locaux de l'AP-HP
- Respecter les systèmes de sécurité physique mis en place à l'AP-HP, en particulier fermer systématiquement à clé s'il le peut, les portes derrière lui, même en cas d'absence de courte durée
- Assurer la protection physique du matériel mis à sa disposition
- Restituer tous les objets permettant l'accès physique aux infrastructures et prêtés par l'AP-HP durant la prestation du TITULAIRE DE MARCHÉ (cartes, clés, etc.) à la fin de l'intervention
- Ne réaliser aucune copie ou duplicata des moyens d'accès mis à disposition
- Ne pas entraver le fonctionnement des équipements opérationnels et ceux de sécurité.

Dans le cas des opérations de maintenance (par exemple, réparation matérielle), le TITULAIRE DE MARCHÉ doit transmettre au préalable à l'AP-HP un descriptif précisant les dates, la nature des opérations à effectuer et les noms des intervenants.

Dans le cas de la livraison d'une solution ou de matériel (par exemple : stock informatique, papiers, mobilier), il est toléré que l'accès du bâtiment soit provisoirement ouvert. Le personnel de l'AP-HP, à défaut le TITULAIRE DE MARCHÉ, est chargé de veiller à la fermeture systématique du bâtiment dès la livraison terminée.

Seul le Personnel affecté aux missions définies dans le cadre du marché peut avoir accès aux clés, codes, matériels ou locaux utilisés pour assurer la protection physique des informations et ressources informatiques appartenant à l'AP-HP.

Chaque membre du personnel du TITULAIRE DE MARCHÉ ayant accès à ces clés ou codes s'engage à les garder secrets, à ne pas les dévoiler ou les laisser à la disposition des tiers.

De même, toujours afin d'assurer la sécurité des biens et des personnes, l'AP-HP limite l'accès à certaines zones sensibles au moyen d'un système de contrôle par badge donnant lieu à un traitement de données à caractère personnel.

Au cours de ses visites dans les locaux de l'AP-HP, le personnel du TITULAIRE DE MARCHÉ ne peut être accompagné d'un tiers ou d'un partenaire du TITULAIRE DE MARCHÉ sans accord écrit préalable du responsable de l'AP-HP ou du responsable du site concerné.

### 3.2 Vidéoprotection

Afin d'assurer la sécurité des biens ou des personnes, certains sites ou lieux sensibles ont été équipés de système de vidéoprotection. Le TITULAIRE DE MARCHÉ reconnaît être informé que de tels systèmes sont mis en place dans les sites sensibles. Le TITULAIRE DE MARCHÉ, mais également à tout opérateur économique intervenant pour le compte ou en partenariat avec le TITULAIRE DE MARCHÉ (cotraitants et sous-traitants notamment), informent ses préposés de la mise en œuvre de ces traitements par l'AP-HP. L'AP-HP s'engage à respecter la législation applicable à ce type d'équipement.



### 3.3 Connexion du matériel du TITULAIRE DE MARCHÉ sur le réseau

Dans la majorité des cas, l'utilisation de matériels informatiques fournis par l'AP-HP doit être privilégiée.

Dans le cas où le TITULAIRE DE MARCHÉ aurait besoin, pour l'exécution de sa prestation, de connecter des matériels informatiques lui appartenant sur le réseau de l'AP-HP, cette connexion est possible aux conditions suivantes :

- Le respect de la Charte d'Utilisation du Système d'Information annexe n°16 du règlement intérieur
- Le respect des différents Politiques Techniques de Sécurité
- L'intégration du matériel au domaine Active Directory
- La présence d'un antivirus à jour et à même de récupérer au moins 1 fois toutes les 24h les dernières signatures antivirales
- L'usage d'un système d'exploitation dans une version maintenue et à jour des correctifs de sécurité et à même de récupérer et d'installer au moins 1 fois par semaine les derniers correctifs de sécurité
- Le respect des contraintes d'adressage MAC/IP
- Cette connexion ne doit en aucune manière avoir un impact sur les performances, la disponibilité, l'intégrité et la confidentialité du Système d'Information de l'AP-HP
- Le matériel doit se connecter au réseau de l'AP-HP par les prises habituelles (Switch, prises RJ45, etc.). Les connexions à l'aide de modem sont interdites.

Le TITULAIRE DE MARCHÉ garantit que son matériel ne présente aucun risque de compromission ou d'infection par un code informatique malveillant, du réseau informatique de l'AP-HP.

Le TITULAIRE DE MARCHÉ s'engage à ne connecter aucun matériel informatique sans l'accord explicite et écrit de l'AP-HP.

## 4 ACCES LOGIQUES

---

### 4.1 Généralités

Tout accès logique au Système d'Information de l'AP-HP nécessite au préalable :

- L'attribution par la DSI d'un compte utilisateur Active Directory, actif pour le temps exclusif de la prestation et / ou de la connexion
- Dans les cas exigés par la réglementation, attribution éventuelle de moyens d'authentification forte de type carte à puce, de façon nominative et pour le temps exclusif de la prestation.

Ces comptes utilisateurs peuvent être nominatifs (individuels) ou exceptionnellement collectifs si une impossibilité technique avérée interdit l'utilisation des comptes nominatifs. Tout accès logique à un système comportant des données nominatives de santé doit être individuel et nominatif.

## Règles de sécurité du Système d'Information applicables aux titulaires de marché de l'AP-HP

Le TITULAIRE DE MARCHÉ s'engage à ne pas entraver et à ne pas contourner la mise en œuvre et l'action de l'ensemble des moyens techniques de l'AP-HP permettant le contrôle des accès autorisés et empêchant les accès non autorisés à son système d'information.

### 4.2 Sécurité des accès logiques

L'AP-HP veille à ce que la sécurité des accès soit conforme aux lois et règlements relevant du domaine informatique (code de la défense, informatique et Libertés, fraude informatique).

L'AP-HP met à disposition de chaque préposé du TITULAIRE DE MARCHÉ devant d'accéder au système d'information :

- Un identifiant personnel et nominatif, un mot de passe fixe et un générateur de mot de passe à usage unique pour l'authentification forte en cas d'accès à distance.

Il appartient au TITULAIRE DE MARCHÉ de s'assurer de la bonne utilisation des moyens d'identification et d'authentification qui lui ont été fournis, et en particulier :

- Garantir que ces codes d'accès ne sont accessibles qu'aux personnels autorisés
- S'assurer de la mise à jour régulière des personnels autorisés, notamment suite à des départs éventuels de préposés du TITULAIRE DE MARCHÉ. Les accès adéquats devront être révoqués en cas de cessation du besoin et / ou de départ du personnel concerné ;
- Traiter ces informations de connexion comme des informations confidentielles ;
- Assurer de façon générale la protection contre tout accès non autorisé par tous les moyens adéquats (protection périmétrique, protection physique, etc.).

Le TITULAIRE DE MARCHÉ s'engage à :

- Faire respecter la protection, la non-divulcation et le non-partage du mot de passe des intervenants qui doivent en assurer une utilisation strictement personnelle. Le mot de passe est inaccessible et doit être suffisamment robuste
- Ne pas user de leur droit pour accéder à des applications, à des données ou à un compte informatique autres que ceux qui leur auront été attribués ou pour lesquels ils ont reçu l'autorisation d'accès
- Ne pas user, par quelque moyen que ce soit, du droit d'accès d'un autre utilisateur
- Ne pas altérer ou détruire des traces ou preuves relatives à des actions ou des événements sur les Systèmes d'Information de l'AP-HP, le concernant ou non
- Ne pas entraver le fonctionnement des équipements opérationnels et ceux de sécurité et dans tous les cas ne pas porter atteinte à la production informatique de l'AP-HP.

Le Personnel du TITULAIRE DE MARCHÉ doit avertir l'AP-HP de tous les dysfonctionnements constatés et/ou de toutes anomalies générées de son fait ou ne le concernant pas mais relevant de la sécurité, qu'il aurait pu observer lors de l'exécution de ses prestations. A cet égard, la procédure d'alerte consiste à prévenir par tout moyen et dans les plus brefs délais l'AP-HP, qui s'attachera à isoler le dysfonctionnement.

### 4.3 Protection contre les logiciels malveillants

Toutes les solutions, qu'elles soient logiques ou physiques, doivent s'intégrer dans la stratégie antivirale de l'AP-HP. Les machines introduites sur le réseau devront avoir une protection antivirale à jour (dernière version disponible de la base de signatures) de façon à éviter la contamination des SI ; étant noté que l'utilisation d'un quelconque outil ou matériel sur le réseau est interdite, sauf accord préalable de l'AP-HP.

De même, tous les supports d'informations (disquettes, clés USB, CD-ROM, etc.) devront avoir été analysés, en présence d'un agent de l'AP-HP, par un antivirus à jour, chaque fois qu'ils doivent être utilisés sur les matériels de l'AP-HP. Le TITULAIRE DE MARCHÉ s'engage à procéder de même pour l'utilisation de tels supports sur son propre matériel.

Lorsque le TITULAIRE DE MARCHÉ intervient sur site, l'AP-HP se réserve le droit d'installer l'antivirus institutionnel sur les machines utilisées par le TITULAIRE DE MARCHÉ dans le cadre de sa prestation afin d'effectuer le scan de chaque poste et des supports d'information.

## 5 TELEMAINTENANCE

---

### 5.1 Généralités

La télémaintenance est nécessaire au bon maintien en condition opérationnelle de beaucoup d'équipements utilisés par l'AP-HP.

Elle se divise en 2 cas d'utilisation en fonction du type de contrat :

- Cas 1 : le TITULAIRE DE MARCHÉ se connecte, depuis l'extérieur de l'AP-HP, à un équipement situé sur le réseau de l'AP-HP ; il s'agit de télémaintenance à proprement parlé
- Cas 2 : le TITULAIRE DE MARCHÉ a positionné sur le réseau interne de l'AP-HP un équipement qui envoie des informations techniques (logs, traces, alertes, etc.) à un équipement du TITULAIRE DE MARCHÉ situé en dehors du réseau de l'AP-HP. Ce cas d'usage s'apparente à de la supervision.

Chaque opération de maintenance fait l'objet d'un descriptif précisant les dates, la nature des opérations et les noms des intervenants, transmis à l'AP-HP.

### 5.2 Connexion depuis l'extérieur

Aucun accès par modem n'est autorisé : tous les accès au système d'information de l'AP-HP depuis l'extérieur devront passer par les équipements de sécurité validés par l'AP-HP.

De plus :

- Aucun accès en télémaintenance ne doit être ouvert en permanence

## Règles de sécurité du Système d'Information applicables aux titulaires de marché de l'AP-HP

- Tout accès en télémaintenance sur un équipement production doit passer par une ouverture manuelle de l'accès, charge à l'AP-HP de déterminer le workflow optimal de gestion des demandes d'accès
- L'ouverture d'un accès en télémaintenance doit avoir une durée limitée à la durée de l'intervention
- Il est nécessaire de tracer nominativement les personnes du TITULAIRE DE MARCHÉ qui accèdent en télémaintenance.

En cas de télémaintenance permettant l'accès à distance aux ressources du SI de l'AP-HP, le TITULAIRE DE MARCHÉ devra mettre en œuvre tous les moyens pour :

- Obtenir l'accord préalable de l'AP-HP avant chaque opération de télémaintenance dont il prendrait l'initiative. En particulier les accès à la production sont strictement interdits, sauf accord explicite de la part de la DSI. Il en va de même pour les environnements d'intégration
- Prendre toutes dispositions afin de permettre à l'AP-HP d'identifier la provenance de chaque intervention extérieure
- Transmettre systématiquement au chef de projet ou responsable du système un rapport de télémaintenance retraçant les opérations menées, les modifications réalisées sur l'environnement de production et leurs impacts éventuels, et ce quels que soient les composants modifiés (système, applications, middlewares, réseaux)
- S'assurer de l'intégrité de son poste, de la mise à jour de celui-ci par rapport aux derniers patches sécurité et protection contre les codes malveillants (antivirus, antimalware ...)
- Ne pas se connecter à des sources concurrentes potentiellement compromettantes telles qu'Internet, autres réseaux d'accès distant, etc.
- Mettre en application l'ensemble des pratiques permettant d'assurer la sécurité de l'accès distant et des outils associés, et se plier aux contraintes techniques imposées par la DSI, notamment sur les moyens techniques de chiffrement des communications à utiliser pour éviter la transmission des données en clair.

En particulier, l'accès en télémaintenance par le TITULAIRE DE MARCHÉ à un serveur de production contenant des données réelles doit être une exception. L'accès en télémaintenance à un serveur de tests ou de préproduction doit être privilégié, afin de réaliser les opérations techniques qui seront ensuite répercutées sur l'environnement de production. Tout accès en direct à un serveur de production doit avoir été validée au préalable par l'AP-HP par écrit (mail de confirmation par exemple). Il peut d'agir d'accès justifiés par l'urgence de l'intervention technique. Tout manquement à cette règle engage la responsabilité juridique du TITULAIRE DE MARCHÉ.

L'utilisation des outils de prise de main à distance par le TITULAIRE DE MARCHÉ doit s'entourer de précautions afin de garantir la transparence dans leur emploi et la confidentialité des données auxquelles le gestionnaire technique accédera par ce moyen, dans la stricte limite de ses besoins :

- Les mots de passe de l'utilisateur assisté ne doivent pas être communiqués au téléassistant
- La télémaintenance du poste de travail doit s'effectuer de manière visuelle par affichage partagé entre l'utilisateur et le téléassistant. L'utilisateur doit être en mesure de voir les opérations effectuées par le téléassistant

## Règles de sécurité du Système d'Information applicables aux titulaires de marché de l'AP-HP

- L'opération de télémaintenance sur le poste de travail de l'utilisateur doit respecter le consentement préalable de ce dernier. Elle ne doit être possible qu'après acceptation explicite de l'utilisateur (dans le cas d'une offre d'assistance) ou à l'initiative de ce dernier (demande d'assistance)
- La télémaintenance ne doit être réalisée que par des personnels dûment autorisés à le faire.

La durée d'indisponibilité de l'accès en télémaintenance mis à disposition du TITULAIRE DE MARCHÉ qui relèverait de la seule responsabilité de l'AP-HP, n'est pas décomptée des engagements de service du TITULAIRE DE MARCHÉ pour les opérations relevant de la télémaintenance.

## 6 SPECIFICITE DANS LES INTERVENTIONS

---

### 6.1 Généralités

Toute intervention sur le SI de l'AP-HP, que ce soit à distance ou sur site, présente des risques inhérents de perturbation dans le fonctionnement des applications.

### 6.2 Engagements du TITULAIRE DE MARCHÉ

La récupération des flux et autres actions visant à tester la robustesse des Systèmes d'Information sont interdites (excepté en cas de demande préalable et explicite de l'AP-HP : audit, tests d'intrusion, tests de montée de charge, validation de performance, etc.).

Par ailleurs, le TITULAIRE DE MARCHÉ s'engage à ne pas se servir du réseau de l'AP-HP pour présenter une solution ou procéder à de l'avant-vente. Pour de telles démonstrations, il devra mettre en place sa propre architecture.

En particulier, il est strictement interdit au TITULAIRE DE MARCHÉ d'utiliser le réseau de l'AP-HP afin de procéder à une démonstration (par exemple de la nouvelle version d'un progiciel déjà détenu par l'APHP, ceci n'étant qu'un exemple) sans avoir obtenu par écrit de l'AP-HP une autorisation.

### 6.3 Incidents

Dans le cadre de la prévention des attaques informatiques, le TITULAIRE DE MARCHÉ et l'AP-HP identifient un ou plusieurs contacts techniques et décisionnels. Pour les prestations revêtant un caractère essentiel à la fourniture du service public vital pour le fonctionnement l'AP-HP, ces contacts sont joignables 24/24, 7/7, tous les jours de l'année.

Le TITULAIRE DE MARCHÉ s'engage à informer immédiatement l'AP-HP de tout événement pouvant affecter la disponibilité, l'intégrité, la pérennité, la confidentialité ou la perte d'informations de l'AP-HP qu'il détient, auxquelles il accède où qu'il manipule.

Le TITULAIRE DE MARCHÉ et l'AP-HP conviennent conjointement d'une définition des procédures de remontée d'incident de sécurité et de la marche à suivre si un incident de sécurité survient.

## 7 PRESTATIONS ET MAINTIEN EN CONDITION DE SECURITE

---

### 7.1 Informations quant aux risques

Le TITULAIRE DE MARCHÉ veille à informer aussi souvent que nécessaire l'AP-HP des failles de sécurité, de façon à permettre à l'AP-HP de prendre les actions préventives ou correctives requises.

Le TITULAIRE DE MARCHÉ s'engage à alerter l'AP-HP sans délai en cas de détection de risque critique pouvant affecter la disponibilité, l'intégrité et la confidentialité de ses prestations.

### 7.2 Homologation de sécurité

Conformément à la politique de sécurité de l'Etat et la politique de sécurité du ministère des affaires sociales, l'AP-HP met en œuvre une démarche d'intégration de la sécurité dans les projets et procède à une homologation de sécurité.

Le TITULAIRE DE MARCHÉ produit les procédures d'exploitation de sécurité de son système :

- La procédure de gestion des incidents de sécurité
- La procédure de gestion des comptes d'accès
- Le modèle d'habilitation et la procédure de gestion des habilitations
- Les procédures sécurisées d'arrêt de et redémarrage des machines
- Les procédures de contrôles des installations logiciels
- La gestion des traces d'audit et l'archivage des journaux d'audit
- Les procédures de sauvegarde des systèmes et de données.

### 7.3 Téléservices de l'administration électronique

Pour les prestations destinées à être le support de téléservices, voire offrir des téléservices, entrant dans le champ de l'ordonnance 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives (Cf. Décret 2010-112 du 2 février 2010 et l'arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité) et conformément au Référentiel Général de Sécurité, l'AP-HP procède à une homologation de sécurité au plus tard en phase de Vérification d'Aptitude (VA) sauf accord entre les parties. Le TITULAIRE DE MARCHÉ s'engage à fournir les éléments nécessaires à cette homologation et à procéder le cas échéant aux adaptations nécessaires.

### 7.4 Mises à jour

Sur ordre de l'AP-HP, et selon une procédure à définir entre les parties intégrant un délai maximum d'installation, le TITULAIRE DE MARCHÉ procède à l'installation des mises à jour de sécurité des logiciels et progiciels utilisés, après avoir procédé aux tests permettant de vérifier qu'elles ne généreront pas d'interruption de l'accès, d'indisponibilité ou une dégradation des performances ou des fonctions.

# Règles de sécurité du Système d'Information applicables aux titulaires de marché de l'AP-HP

Le TITULAIRE DE MARCHÉ prend en compte la mise à jour de la liste des risques effectuée et communiquée par l'AP-HP.

Le TITULAIRE DE MARCHÉ s'engage à mettre à jour la sécurité de la SOLUTION dans le respect des règles d'intégrité et de confidentialité.

## 7.5 Gestion des vulnérabilités techniques

L'AP-HP procède à une recherche périodique des vulnérabilités techniques de son système d'information. Elle utilise le référentiel COMMON VULNERABILITY SCORING SYSTEM (CVSS) en version 2.0 du NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), et notamment le guide de mise en œuvre « CVSS IMPLEMENTATION GUIDANCE » pour caractériser les vulnérabilités techniques.

### Vulnérabilités techniques des prestations

Les vulnérabilités techniques, qui ont les caractéristiques suivantes **sont considérées comme une anomalie bloquante** :

1. Vecteur d'attaque (ACCESS VECTOR) = Réseau (NETWORK)
2. Complexité d'exploitation (ACCESS COMPLEXITY) inférieure ou égale à moyen (MEDIUM)
3. Authentification = non nécessaire (NONE)
4. Impact sur la confidentialité, l'intégrité ou la disponibilité supérieure ou égale à partiel (PARTIAL).

Les vulnérabilités techniques de la SOLUTION qui auraient les caractéristiques suivantes Sont considérées comme une anomalie majeure :

1. Vecteur d'attaque (ACCESS VECTOR) = réseau adjacent (ADJACENT NETWORK)
2. Quelle que soit la complexité d'exploitation
3. Avec ou sans authentification
4. Impact sur la confidentialité, l'intégrité ou la disponibilité supérieure ou égale à partiel (PARTIAL).

Les autres vulnérabilités techniques sont considérées comme des incidents mineurs.

Leur résolution suit les règles de gestion des anomalies et incidents telles que décrites dans le marché.

### Vulnérabilités techniques de l'environnement

L'AP-HP met en œuvre un plan de maintenance préventive des composants technologiques sous-jacent aux prestations (Systèmes d'exploitation, base de données...) en appliquant périodiquement les correctifs de sécurité publiés par les éditeurs.

La période de mise à jour par défaut est le trimestre excepté, pour les vulnérabilités techniques, dont le vecteur d'attaque (ACCESS VECTOR) est égal à Réseau (NETWORK) et l'authentification est non nécessaire (NONE), qui doivent être comblées sans délai (correctif de sécurité ou mesure d'atténuation).

Le TITULAIRE DE MARCHÉ garantit la bonne exécution de ses prestations dans le cadre de ce plan de maintenance. En cas de dysfonctionnement de ses prestations, l'origine de l'incident est imputable au TITULAIRE DE MARCHÉ et non pas aux composants technologiques sous-jacents. Leur résolution suit alors les règles de gestion des anomalies et incidents définies dans le marché.

## 8 AUDITS

---

### 8.1 Audit par le TITULAIRE DE MARCHÉ

#### **Agrément relatif à l'auditeur**

L'auditeur proposé par le TITULAIRE DE MARCHÉ doit être agréé par l'AP-HP. Aucun auditeur ne peut être imposé à l'AP-HP, dans la mesure où il peut présenter un risque de partialité. Il doit être reconnu en tant qu'auditeur indépendant, c'est-à-dire indépendant du TITULAIRE DE MARCHÉ, ayant une qualification adéquate, et libre de fournir les détails de ses remarques et conclusion d'audit à l'AP-HP.

#### **Agrément relatif à l'audit**

La réalisation de l'audit du TITULAIRE DE MARCHÉ est soumise à l'agrément de l'AP-HP. Afin de permettre à l'AP-HP de procéder à l'agrément de l'audit, le TITULAIRE DE MARCHÉ fournit à l'AP-HP une lettre de cadrage de l'audit par « lettre recommandée avec avis de réception postale » (ou équivalent) mentionnant notamment : le périmètre des investigations, les limitations, les moyens techniques mis en œuvre, la date proposée, la durée, et toutes informations jugées utiles. Ce document retrace donc notamment l'ensemble des moyens techniques, outils, méthodes... qui sont mis en œuvre lors de l'audit.

L'agrément ne pourra être délivré que dans la mesure où :

- L'audit du TITULAIRE DE MARCHÉ ne suscite pas d'impact sur la production de l'AP-HP ni sur le bon fonctionnement de ses services et services associés
- Le TITULAIRE DE MARCHÉ respecte un délai de prévenance de deux (2) mois pour soumettre l'agrément de l'audit et de l'auditeur à l'AP-HP.

#### **Modalités complémentaires de délivrance de l'agrément**

A réception de l'ensemble des éléments nécessaires pour engager la procédure d'agrément, l'AP-HP dispose d'un (1) mois pour se prononcer sur l'agrément ou le rejet de la demande d'audit.

#### **Modalités liées à la réalisation de l'audit**

Le TITULAIRE DE MARCHÉ prend en charge l'intégralité des coûts de l'audit, dont notamment la rémunération de l'auditeur interne ou externe, la prise en charge des coûts liés à la mobilisation de ressources humaines internes aux taux horaires desdites personnes...



# Règles de sécurité du Système d'Information applicables aux titulaires de marché de l'AP-HP

La personne Publique se réserve la faculté de modifier la date prévue de l'audit :

- Dans la limite de deux (2) reports par demande d'audit
- Avec report de la date de l'audit dans un délai maximal d'un (1) mois suivant la date prévisionnelle agréée.

## **Responsabilité liée à l'audit**

Le TITULAIRE DE MARCHÉ engage son entière responsabilité au titre des préjudices qui pourraient naître au détriment de l'AP-HP à l'occasion de l'audit et qui résulteraient, notamment, d'une faute, erreur ou omission de l'auditeur.

## **Confidentialité liée aux résultats de l'audit**

Le TITULAIRE DE MARCHÉ s'engage à respecter la plus stricte confidentialité au titre des éléments qu'il serait amené à connaître dans le cadre de l'audit. Il s'engage notamment à ne pas divulguer les résultats de l'audit réalisé à des tiers au marché concerné par l'audit.

## **8.2 Audit par l'AP-HP**

Sous réserve d'un préavis de dix (10) jours ouvrés, l'AP-HP se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect par le TITULAIRE DE MARCHÉ de ses obligations au titre du marché, notamment par le biais d'un audit.

Le TITULAIRE DE MARCHÉ s'engage à répondre aux demandes d'audit de l'AP-HP et effectuées par l'APHP elle-même ou par un tiers de confiance qu'elle aura sélectionné, reconnu en tant qu'auditeur indépendant, c'est-à-dire indépendant du TITULAIRE DE MARCHÉ, ayant une qualification adéquate, et libre de fournir les détails de ses remarques et conclusion d'audit à l'AP-HP.

Les audits doivent permettre une analyse du respect du présent marché et de la loi Informatique et Libertés, notamment : par la vérification de l'ensemble des mesures de sécurité mises en œuvre par le TITULAIRE DE MARCHÉ, par la vérification des journaux de localisation des données, de copie et de suppression des données, par l'analyse des mesures mises en place pour supprimer les données, pour prévenir toutes transmissions illégales de données à des juridictions non adéquates ou pour empêcher le transfert de données vers un pays non autorisé. L'audit doit enfin pouvoir permettre de s'assurer que les mesures de sécurité et de confidentialité mises en place ne peuvent être contournées sans que cela ne soit détecté et notifié.

Il est toutefois entendu qu'un tel audit ou toute autre forme de contrôle/vérification ne peut en aucun cas porter sur les documents financiers et/ou comptables du TITULAIRE DE MARCHÉ ou sur les documents relatifs aux membres du personnel du TITULAIRE DE MARCHÉ (sauf accord préalable et éclairé de ces derniers). L'AP-HP s'engage à respecter les obligations de confidentialité qui lui incombent au titre des présentes ainsi que les règles d'accès et de sécurité en vigueur dans les locaux du TITULAIRE DE MARCHÉ et se porte fort du respect de ces règles par les membres de son personnel et/ou auditeur externe.

## 9 TRACABILITE

---

Tout accès au SI de l'AP-HP est tracé, conformément aux lois informatiques et Liberté.

Les opérations de télémaintenance font l'objet d'une traçabilité nominative détaillée conforme à la déclaration à la commission nationale informatique et libertés (CNIL) enregistrée sous le n° 1756671 v 0 du 07 avril 2014.

Une traçabilité générale inhérente à l'usage des systèmes d'information conforme à la déclaration à la commission nationale informatique et libertés enregistrée sous le n° 1562250 v 1 le 21 mars 2012 est mise en œuvre par l'AP-HP.

Le TITULAIRE DE MARCHÉ reconnaît être informé que de tels systèmes sont mis en place. Le TITULAIRE DE MARCHÉ, mais également tout opérateur économique intervenant pour le compte ou en partenariat avec le TITULAIRE DE MARCHÉ (cotraitants et sous-traitants notamment), informe ses préposés de la mise en œuvre de ces traitements par l'AP-HP. L'AP-HP s'engage à respecter la législation applicable dans ce domaine.

### 9.1 Traçabilité des accès pour les comptes génériques

Il appartient au TITULAIRE DE MARCHÉ, dans le cas de l'attribution d'un compte utilisateur générique (c'est-à-dire affecté au TITULAIRE DE MARCHÉ et non pas nominativement à un ou plusieurs de ses préposés) de gérer la traçabilité des accès.

L'AP-HP doit, sur simple demande, pouvoir disposer de l'historique nominatif de l'utilisation de cet accès générique, pour savoir quel préposé du TITULAIRE DE MARCHÉ a utilisé cet accès, à quelles dates et heures, pour quelle durée et pour quelle action.

## 10 ASPECTS JURIDIQUES

---

### 10.1 Responsabilité

Conformément à la loi, le TITULAIRE DE MARCHÉ est responsable de tous les dommages corporels, matériels et immatériels, directs ou indirects, trouvant leur origine aussi bien dans une exécution fautive, même partielle ou une mauvaise exécution ou une inexécution des obligations mises à sa charge dans la présente charte.

Le TITULAIRE DE MARCHÉ est seul responsable du respect des présents engagements et de leur mise en œuvre ainsi que de leur respect par son Personnel.

## Règles de sécurité du Système d'Information applicables aux titulaires de marché de l'AP-HP

Nonobstant sa responsabilité contractuelle, le TITULAIRE DE MARCHÉ est informé que selon la faute commise, des sanctions civiles (par exemple pour atteinte au droit à l'image d'un tiers) et/ou pénales (par exemple pour intrusion frauduleuse dans les SI ou pour violation du secret professionnel) pourront être prononcées par les juges.

### 10.2 Respect des lois en vigueur

Le TITULAIRE DE MARCHÉ s'engage non seulement au respect de la présente charte, mais déclare également connaître et respecter la réglementation en vigueur et notamment à titre non limitatif :

- La loi 78-17 du 6 janvier 1978 modifiée par la loi du 4 août 2004 relative à l'informatique, aux fichiers et aux libertés et ses textes d'application
- Les dispositions du code pénal relatives à la fraude informatique (articles 323-1 à 323-7 du Code pénal)
- Les dispositions du code civil relatives aux atteintes aux droits de la personne (notamment atteintes à l'intimité de la vie privée et au droit à l'image)
- Les dispositions du code pénal relatives aux atteintes aux droits de la personne (notamment, atteintes à la vie privée, au secret des correspondances privées, atteintes au secret professionnel et atteintes résultant de fichiers ou de traitements informatiques) ;
- Les dispositions du code de la propriété intellectuelle relatives au droit d'auteur (les logiciels, toutes les œuvres de l'esprit quelle que soit leur nature, les bases de données), aux brevets, aux marques et aux dessins et modèles
- Les dispositions relatives au Référentiel Général de Sécurité (RGS)
- La Politique de Sécurité des Systèmes d'Information de l'Etat.

La présente charte est de plus conforme aux normes en vigueur :

- La norme ISO 27 000
- Les bonnes pratiques recommandées par l'ANSSI, et en particulier le guide d'hygiène
- Les bonnes pratiques recommandées par l'ASIP.

### 10.3 Intitulé des clauses

Les intitulés portés en tête de chaque article ne servent qu'à la commodité de la lecture et ne peuvent en aucun cas être le prétexte d'une quelconque interprétation ou dénaturation des clauses sur lesquelles ils portent.

### 10.4 Invalidité d'une clause

Si une ou plusieurs stipulations de la présente charte sont tenues pour non valides ou déclarées telles en application d'une loi, d'un règlement ou à la suite d'une décision définitive d'une juridiction compétente, les autres stipulations conserveront leur pleine validité sauf si elles présentent un caractère indissociable avec la stipulation non valide.

### 10.5 Exceptions

## Règles de sécurité du Système d'Information applicables aux titulaires de marché de l'AP-HP

Chaque cas d'exception appelant une dérogation à la présente charte devra systématiquement être soumis à l'AP-HP pour identification, validation et suivi.

# Fiche de déclaration d'un accès au SI de l'AP-HP

Création ☐ Suppression ☐ Modification ☐

\* Champ obligatoire

## Coordonnées du déclarant

Nom et prénom ou raison sociale\* \_\_\_\_\_

Sigle (facultatif) \_\_\_\_\_ SIRET | | | | | | | | | | | | | | | |

Service \_\_\_\_\_ FINESS géographique | | | | | | | | | | | | | | | |

Adresse\* \_\_\_\_\_

Code postal\* \_\_\_\_\_ Ville\* \_\_\_\_\_ Tél.\* \_\_\_\_\_

Mèl\* \_\_\_\_\_ FAX \_\_\_\_\_

Référence du marché/convention\* \_\_\_\_\_ Date de début\* \_\_\_\_\_

\_\_\_\_\_ Date de fin\* \_\_\_\_\_

Personne à contacter au sein de l'organisme déclarant si un complément d'information doit être demandé :

Nom et prénom\* \_\_\_\_\_

Mèl\* \_\_\_\_\_

## Coordonnées du bénéficiaire

\* Champ obligatoire

Monsieur ☐ Madame ☐

Nom et prénom\* \_\_\_\_\_

Service \_\_\_\_\_

Adresse\* \_\_\_\_\_

Code postal\* \_\_\_\_\_ Ville\* \_\_\_\_\_ Tél.\* \_\_\_\_\_

Mèl\* \_\_\_\_\_ FAX \_\_\_\_\_

Identifiant de connexion

| | | | | | | | | | | | | | | | Zone réservée à l'AP-HP

## Mode d'accès demandé

Réseau filaire ☐ WIFI AP-HP ☐ Accès à distance ☐

Identifiant SYMANTEC VIP principal\*

| | | | | | | | | | | | | | | |

Identifiant SYMANTEC VIP de secours

| | | | | | | | | | | | | | | |

## Identification de l'équipement tiers

Marque \_\_\_\_\_ Modèle \_\_\_\_\_ S/N \_\_\_\_\_

Système d'exploitation \_\_\_\_\_ Antivirus \_\_\_\_\_

Adresse MAC | | | | | | | | | | | | | | | | Nom de machine \_\_\_\_\_

## Justificatif à joindre à ce formulaire dûment complété et signé

Photocopie d'un justificatif d'identité du bénéficiaire : carte d'identité, passeport, permis de conduire, carte de séjour ou de  
résident

Justification de la demande d'accès :
Je certifie exactes les informations mentionnées dans le présent formulaire. (Il est rappelé que les fraudes et tentatives de fraude sont passibles de sanctions pénales et peuvent conduire à la suspension de l'instruction ou au retrait des droits dont le bénéfice est demandé).
Signature du « représentant légal » et cachet du déclarant

### Engagement du Bénéficiaire

Je soussigné \_\_\_\_\_

certifie avoir pris connaissance du règlement intérieur de l'AP-HP -notamment son annexe n°16  
intitulé « Charte de bon usage du système d'information de l'AP-HP »- et des règles de sécurité  
du Système d'Information applicables aux TITULAIRES DE MARCHE de l'AP-HP datée de  
novembre 2016 et m'engage à les respecter et à m'y conformer strictement.

A \_\_\_\_\_ le, \_\_\_\_\_

Signature du Bénéficiaire précédée de la mention manuscrite « lu et approuvé »

La copie du justificatif d'identité du bénéficiaire est conservée le temps de l'instruction de la demande puis détruite.  
Les opérations de télémaintenance font l'objet d'une traçabilité nominative détaillée conforme à la déclaration à la  
commission nationale informatique et libertés (CNIL) enregistrée sous le n° 1756671 v 0 du 07 avril 2014.

Conformément à la loi Informatique et Libertés du 6 janvier 1978 modifiée par la loi du 6 Août 2004, vous disposez  
d'un droit d'accès, de rectification, de suppression et d'opposition aux données personnelles vous concernant. Pour  
ce faire il vous suffit, en justifiant de votre identité, d'écrire :

- Par voie postale : Assistance Publique – Hôpitaux de Paris -Direction des Systèmes d'Information - Mission  
Sécurité - Rothschild – Pavillon 2 – 3ème étage – bureau 304 - 33 Boulevard Picpus – 75012 Paris
- Par courrier électronique : dsi-securite-contacts@aphp.fr.