

CHARTRE SECURITE DU SYSTEME D'INFORMATION

Pouvoir Adjudicateur

Mipih
12 rue Michel Labrousse
CS 93668
31036 Toulouse Cedex 1

N° de marché :

Accepté sans réserve à, le

Cachet de l'entreprise, Nom - Prénom et qualité du signataire

SOMMAIRE

Article 1. Définitions	4
Article 2. Objet de la charte	4
Article 3. Domaine d'application – Périmètre.....	5
Article 4. Documents de référence	5
Article 5. Règlementation en vigueur	5
Article 6. Règles générales d'utilisation des moyens de technologie de l'information et communication	7
6.1 Dispositions générales.....	7
6.1.1 Règles générales d'utilisation et de sécurité	7
6.1.2 Ressources informatiques	8
6.1.3 Prévention de l'intégrité des systèmes informatiques	8
6.1.4 Surveillance	8
6.2 Dispositions spécifiques au SI-DonnéesSanté	9
Article 7. Engagements spécifiques du Titulaire	9
7.1 Défauts et règlement des différends.....	9
7.2 Etats de l'art	9
7.3 Labels et certificats	9
7.4 Confidentialité	9
7.5 Transfert d'information	10
7.6 Accès physiques	11
7.7 Accès logiques.....	12
7.8 Signalements de sécurité.....	12
7.9 Dispositifs connectés au Système d'Information	13
7.9.1 Maintien en condition de sécurité.....	14
7.10 Interventions à distance.....	14
7.11 Règles spécifiques à l'hébergement	16
7.11.1 Hébergement au Mipih.....	16
7.11.2 Hébergement hors Mipih	16
7.12 Destruction des données	16
7.13 Développements réalisés par le Titulaire	17
7.14 Protection des données de test	17



Article 8. Audits, traçabilité et contrôle	17
Article 9. Responsabilité	18
ANNEXE 1. Engagement de confidentialité	19

Article 1. Définitions

Au sens de la présente Charte, les expressions et/ou mots ci-dessous auront la définition suivante :

« **Titulaire** » : Titulaire du présent marché ainsi que ses éventuels sous-traitants dont il fait son affaire et pour lesquels il s'engage.

« **Système d'Information (SI)** » : ensemble des ressources, matérielles et logicielles, des moyens techniques, et 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 du Mipih. Cela inclut entre autres : les logiciels (applications informatiques, systèmes de messagerie électronique, outils bureautiques, systèmes d'exploitation, outils d'administration, utilitaires, bases de données...), le matériel informatique ou bureautique (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 (stockage virtualisé, disques durs, supports USB, ...) et les équipements de production.

« **SI-DonnéesSanté** » : système d'information du Mipih constitué de l'ensemble des ordinateurs, des serveurs, des réseaux, des logiciels, des données immatérielles, dont les données de santé à caractère personnel, et les périphériques nécessaires à l'hébergement de données de santé à caractère personnel.

« **SSI** » : Sécurité des Systèmes d'Information du Mipih.

« **Ressources informatiques** » : moyens informatiques locaux de traitement des données ainsi que ceux auxquels il est possible d'accéder à distance, directement ou en cascade, à partir du réseau administré par ou pour le Mipih.

Article 2. Objet de la charte

La présente charte énonce les exigences du Mipih en termes de sécurité vis-à-vis de ses prestataires externes au titre desquels figure le Titulaire du présent marché, et ayant accès à un ou plusieurs éléments constituant le Système d'Information du Mipih (ci-après « le SI »).

Le présent document a pour objet de définir les conditions et modalités que le Titulaire s'engage à respecter afin d'assurer la sécurité du SI du Mipih (et des SI hébergés) ainsi que de ses données. L'objectif consiste ainsi à éviter que les relations avec le Titulaire ne constituent une faille dans les règles de sécurité informatique définies dans la Politique de Sécurité du Système d'information du Mipih (PSSI).

Sauf mention contraire figurant au titre des présentes, le Titulaire est soumis à une obligation de moyens pour assurer et garantir la sécurité des informations et des ressources appartenant au Mipih, étant entendu que la charge de la preuve lui

incombe. Le Mipih se réserve néanmoins le droit de procéder à toute vérification qui lui paraît utile pour constater le respect de ses obligations.

Un Plan d'Assurance Sécurité (PAS) sera exigé pour certaines prestations.

L'intégralité des obligations incombant au Titulaire au titre du présent document s'applique aux tiers qu'il ferait intervenir pour son compte (sous-traitant notamment), et ce sous son entière responsabilité.

Article 3. Domaine d'application – Périmètre

La présente charte s'applique à tous les marchés conclus par le Mipih dès lors que le Titulaire doit avoir accès à tout ou partie du SI du Mipih. Le présent document est un document contractuel auquel le Titulaire ne peut se soustraire.

La présente charte est applicable à tous les personnels du Titulaire ainsi qu'aux personnels d'autres structures intervenant pour son compte (sous-traitant ...). En aucun cas, et notamment si le Titulaire a recours à la sous-traitance, la responsabilité du Titulaire ne pourra être écartée. Les contrôles des sous-traitants et les éventuelles actions de remédiation en cas de défaut, y compris jusqu'au remplacement, sont à la charge des titulaires.

La présente Charte est annexée au Cahier des Clauses Administratives Particulières (CCAP) du marché et s'impose au Titulaire pendant toute la durée du marché mais également après en ce qui concerne certaines dispositions spécifiques (obligation de confidentialité notamment).

Article 4. Documents de référence

La présente charte s'appuie sur les référentiels et normes et arrêtés en vigueur suivants :

- Normes de la famille ISO/IEC 27000 ;
- Les bonnes pratiques recommandées par l'ANSSI ;
- Les bonnes pratiques recommandées par l'ASIP ;
- Cahier des clauses simplifiées de cybersécurité (Arrêté du 18 septembre 2018 - NOR: ECOP1825228A).

Le Titulaire prend en compte les référentiels et normes listés ci-avant dans le cadre de son intervention.

Article 5. Règlementation en vigueur

Outre les dispositions spécifiquement prévues au présent document, le Titulaire déclare connaître et respecter l'ensemble de la réglementation en vigueur sans qu'il soit besoin que le cahier des charges en fasse mention explicitement et notamment :

- la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et au Règlement (UE) 2016/679 du 27 avril 2016 (RGPD) qui prévoient la tenue de registres des traitements et la documentation des mesures de protection. Le candidat ou titulaire et leurs sous-traitants identifient pro-activement les traitements de données personnelles ou sensibles et aident à la réalisation d'analyses d'impact relative à la protection des données et à la consultation préalable des autorités de contrôle;
- 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 du Mipih quelles que soient leurs natures, les bases de données), aux brevets, aux marques et aux dessins et modèles ;
- les dispositions relatives au Référentiel Général de Sécurité ;
- la Politique de Sécurité des Systèmes d'Information de l'Etat (PSSIE) élaborée par l'ANSSI et l'arrêté du 1er octobre 2015 du Ministre de la Santé portant approbation de la politique de sécurité des systèmes d'information pour les Ministères Chargés des Affaires Sociales (MCAS) précise les dispositions de la PSSIE. Cette PSSIE-MCAS concerne les directions, Services centraux, les services déconcentrés, des ministères chargés des affaires sociales ainsi que les établissements placés sous leurs tutelles. Elle concerne également, par voie contractuelle ou conventionnelle toute personne physique ou morale tierce intervenant dans un système d'information dont l'activité concourt aux missions des MCAS (fournisseurs, prestataires de service, sous-traitants, employés, agents ...).
- le Décret confidentialité n° 2007-960 du 15 mai 2007 fixant les mesures de sécurité relatives à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique et modifiant le code de la santé publique (dispositions réglementaires).
- l'article L1110-4 du Code de la Santé Publique, Modifié par [Ordonnance n°2018-20 du 17 janvier 2018 - art. 2](#)

Le Titulaire s'engage par ailleurs à prendre en compte toute évolution de la législation intervenant pendant la durée de validité du présent marché. Sur demande expresse du Mipih, le Titulaire devra justifier sans délai la mise en conformité avec la nouvelle réglementation.

Article 6. Règles générales d'utilisation des moyens de technologie de l'information et communication

6.1 Dispositions générales

6.1.1 Règles générales d'utilisation et de sécurité

Le Titulaire est responsable de l'usage des ressources informatiques auxquelles il a accès ou qui sont mises à sa disposition dans le cadre de l'exécution du marché. Une utilisation conforme desdites ressources doit ainsi permettre de contribuer à la sécurité générale du SI du Mipih.

En particulier, le Titulaire :

- a interdiction de détourner à des fins personnelles et/ou commerciales tous les moyens mis à sa disposition ;
- doit appliquer toutes les recommandations de sécurité précisées par le Mipih ;
- doit intervenir dans un strict souci de garantir la protection des données auxquelles il a accès ;
- doit suivre toutes les règles et contraintes applicables au Mipih en matière d'installation de logiciels ;
- s'engage à ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou réseaux à travers de matériels dont il a l'usage ;
- ne doit pas tenter de lire, modifier, copier ou détruire des données, informations ou documents autres que ceux dont il a strictement besoin à l'exécution du marché, et ce quand bien même lesdits éléments n'auraient pas été protégés ;
- ne doit pas transmettre sur le réseau vers l'extérieur du Mipih des informations nominatives non protégées.

Au titre du marché, le personnel du Titulaire :

- doit appliquer les recommandations de sécurité de la PSSI du Mipih ;
- doit utiliser son compte d'accès et élaborer des mots de passe sûrs, selon les règles de la PSSI ;
- doit signaler toute tentative de violation de son compte et toute anomalie qu'il peut constater, auprès du responsable sécurité du Mipih (RSSI) ;
- ne doit pas utiliser ou essayer d'utiliser des comptes autres que le sien ou de masquer sa véritable identité ;
- s'engage à ne pas mettre à la disposition d'utilisateurs non autorisés un accès au SI ;
- doit prendre toutes les mesures nécessaires à empêcher l'accès au SI (verrouillage des postes informatiques ...) ;
- doit suivre les règles en vigueur pour toute installation, mise à jour, accès, maintenance,... de logiciel ;
- ne doit pas introduire, intentionnellement, des ressources extérieures qui pourraient porter atteinte à la sécurité du SI ;
- ne doit effectuer aucune action intentionnelle pouvant perturber la disponibilité du SI ;
- ne doit pas installer, intentionnellement, de copie illicite de logiciels ;

- doit assurer la protection des informations auxquelles il accède en appliquant les consignes de sécurité émises par le Mipih, et doit utiliser les outils de sécurité mis en œuvre ;
- ne doit pas tenter de lire, modifier, copier ou détruire des données sans en disposer des droits en relation avec sa mission ;
- doit soigner la qualité des informations transmises, et ne dénigrer ni le Mipih, ni les adhérents ou les clients du Mipih ;
- ne doit pas modifier le contenu d'un message qu'il transmet et dont il n'est pas l'auteur ;
- est tenu par le secret professionnel.

Si dans le cadre de l'exécution du marché le Titulaire est amené à constituer des fichiers tombant sous le coup de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ou du Règlement (UE) 2016/679 du Parlement Européen, il devra strictement se conformer aux obligations de la CNIL en la matière.

6.1.2 Ressources informatiques

Les ressources et les moyens mis à disposition du titulaire par le Mipih sont réservés à l'exécution des prestations objet du marché.

Les ressources informatiques mises à disposition du Titulaire :

- sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à des tiers ;
- peuvent être retirées à tout moment.

Si les ressources informatiques mises à disposition du Titulaire demeurent la propriété du Mipih, le Titulaire en est le garant. A ce titre, le Titulaire met en œuvre toutes les mesures conservatoires nécessaires devant permettre de garantir l'intégrité des ressources (protection contre la détérioration, le vol, les actes de malveillance ...).

Le Titulaire restitue sans délai l'intégralité des ressources informatiques attribuées dès la fin des relations contractuelles avec le Mipih, que celle-ci intervienne à l'issue du marché ou de façon anticipée (résiliation, ...).

6.1.3 Prévention de l'intégrité des systèmes informatiques

Le Titulaire s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement des systèmes informatiques et des réseaux que ce soit par des manipulations anormales du matériel ou par l'introduction de logiciels malveillants connus sous le nom générique de virus.

Tout travail comportant un risque de violation de la règle définie dans le paragraphe précédent, ne pourra être accompli qu'avec l'autorisation expresse du Mipih et dans le strict respect des règles qui auront alors été définies.

6.1.4 Surveillance

Le Titulaire est informé que le Mipih dispose de logiciels lui permettant de suivre le trafic sur le réseau. Il se réserve le droit de contrôler à tout moment l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau.

6.2 Dispositions spécifiques au SI-DonnéesSanté

L'utilisation du SI-DonnéesSanté par le Titulaire est strictement limitée aux besoins du marché. Le Titulaire est responsable de l'usage du SI-Données Santé. Une utilisation conforme des accès doit ainsi permettre de contribuer à la sécurité générale du SI du Mipih.

Au titre du marché, le personnel du Titulaire :

- ne doit pas accéder ni transmettre des données de santé à caractère personnel, sauf pour des raisons techniques justifiées. En ce cas, les accès doivent être tracés. Les transferts de ces données doivent être rendus confidentiels par un moyen de cryptage ;

Article 7. Engagements spécifiques du Titulaire

7.1 Défauts et règlement des différends

Tout au long des processus d'attribution et d'exécution d'un marché, le Mipih peut constater ou découvrir des non-conformités à sa politique de sécurité et des défauts de sécurisation.

Le Mipih apprécie l'enjeu du défaut eu égard à la sensibilité des données manipulées, de leurs volumes, et des conséquences prévisibles si le défaut persiste.

En fonction de cette analyse, ces défauts peuvent avoir comme conséquence le rejet d'une candidature, d'une offre, la non-validation d'aptitude au service régulier, l'ajournement, la suspension ou la résiliation des bons de commandes ou du marché.

7.2 Etats de l'art

La sécurisation des systèmes informatiques dépend de l'évolution des technologies. Il appartient à chaque titulaire de marché de s'aligner sur les standards et référentiels qui concernent les services qu'il propose, utilise ou met à disposition.

7.3 Labels et certificats

Afin de démontrer de manière économique la réalité de leurs efforts pour sécuriser les composants impliqués dans le marché, candidats et titulaires sont invités à présenter des labels et certificats qui permettent à l'acheteur d'avoir un premier niveau d'assurance au cours de l'évaluation d'offres.

7.4 Confidentialité

Si le CCAP applicable fixe le régime des propriétés des prestations et/ou fourniture exécutées et/ou livrées dans le cadre du marché, il est strictement entendu que les supports informatiques et toutes données et informations, quel qu'en soit le support, fournis par le Mipih et tout document de quelque nature qu'il soit résultant de leur traitement demeurent la propriété du Mipih.

Dans l'hypothèse où le Titulaire serait amené à accéder à des données à caractère personnel, il est rappelé que celles-ci sont strictement couvertes par le secret professionnel (article 226-13 du Code Pénal), dans le respect des dispositions de la loi 2018-493 du 20 juin 2018 relative à l'informatique, aux fichiers et aux libertés et du Règlement (UE) 2016/679 du Parlement Européen. Le Titulaire s'engage à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des personnes non autorisées et signaler toute violation de données à caractère personnel. Ces obligations s'imposent également à tout tiers intervenant pour le compte du Titulaire.

Le Titulaire s'engage à respecter et à faire respecter par chacun de ses personnels (et tiers intervenant pour son compte) les obligations suivantes :

- ne prendre aucune copie des documents et supports d'informations confiés, à l'exception de celles strictement nécessaires à l'exécution des prestations dont il a la charge ;
- ne pas divulguer ces documents ou informations à des tiers, qu'il s'agisse de personnes privées ou publiques, physiques ou morales, et à cet effet, mettre en œuvre tout procédé et mesure utile ; prendre toute mesure permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques, notamment de sécurité matérielle, pour assurer la conservation des documents et informations traités ;
- en fin de contrat ou d'intervention, procéder à la destruction de tous les fichiers manuels ou informatisés stockant les informations saisies, et/ou à restituer intégralement les supports d'informations ;
- faire signer à son personnel un engagement individuel de confidentialité (annexe 1)

7.5 Transfert d'information

Les échanges d'information entre le Titulaire et le Mipih répondent à un protocole d'échange formel ; le Titulaire s'engage à mettre en place les moyens permettant de respecter les obligations suivantes et à les faire respecter par ses préposés :

- protéger l'information échangée contre l'interception, la reproduction, la modification, les erreurs d'acheminement et la destruction ;
- la messagerie sera protégée contre les codes malveillants et les échanges ayant besoin d'intégrité et de confidentialité seront chiffrés avec un moyen adapté ; choisir des coursiers de confiance et du mode de transport des informations sensibles :
 - utilisation de contenant à clef, envoi séparé de la clef ;
 - livraison en main propre ;
 - emballage inviolable, permettant de repérer facilement toute tentative d'effraction.

7.6 Accès physiques

Le Titulaire s'engage à strictement respecter les obligations listées ci-après et à les faire respecter par l'ensemble de ses préposés et tiers intervenant pour son compte (sous-traitant, ...) :

- limiter strictement l'accès aux clefs, codes, matériels ou locaux utilisés pour assurer la protection physique des informations et ressources informatiques propriétés du Mipih aux seuls personnels affectés à la mission dans le cadre de l'exécution des prestations objet du marché ;
- accéder aux locaux du Mipih uniquement dans les horaires, jours et périmètre convenus dans le marché et nécessaire à la réalisation de la mission, dans le respect des règles d'accès physique définies par le Mipih ;
- ne pas essayer de s'introduire dans des salles non autorisées ou avec d'autres moyens que ceux mis à disposition dans le cadre du marché ;
- ne pas accéder aux salles machines et salles techniques (informatiques et télécommunications) du Mipih, sauf autorisation écrite spéciale ou accompagné d'un agent du Mipih et si l'objet de la prestation le justifie ;
- ne pas permettre l'accès aux personnes non-autorisées par le Mipih dans les locaux de ce dernier ;
- assurer la protection physique du matériel mis à disposition ; ne réaliser aucune copie ou duplicata des moyens d'accès mis à disposition ;
- ne pas entraver le fonctionnement des équipements opérationnel et de sécurité.

Le Titulaire reconnaît être informé que :

- certains sites sensibles sont équipés de procédés de vidéosurveillance afin d'assurer la sécurité des biens ou des personnes ; le Mipih s'engage à respecter la réglementation relative à cette typologie d'équipement ;
- le Mipih 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. Ainsi, tout personnel du Titulaire ayant une habilitation peut accéder à des lieux déterminés selon le type et le niveau d'habilitation dont il jouit. Le Mipih s'engage à respecter la réglementation relative aux traitement des données à caractère personnel mis en place à cet effet.

Dans le cadre des opérations de maintenance (réparation matérielle ...), le Titulaire transmet préalablement au Mipih un descriptif précisant la date d'intervention, la nature des opérations à effectuer, les noms des intervenants ainsi que les conditions de bon déroulement de la prestation (nécessité pour le Mipih de préparer des documents, logiciels ou matériels).

Dans le cas de la livraison d'une solution ou de matériels (stock informatique, papier, mobilier ...), il est toléré que l'accès du bâtiment puisse être provisoirement ouvert. Le référent technique du Mipih acceptant la livraison ou le Titulaire sous la responsabilité du référent technique du Mipih est chargé de veiller à la fermeture systématique du bâtiment dès la livraison achevée.

7.7 Accès logiques

Tout accès logique au Système d'Information du Mipih nécessite au préalable l'attribution par le Mipih d'un compte utilisateur Active Directory, actif exclusivement le temps de la prestation et ou de la connexion.

Les comptes Active Directory sont nominatifs (individuels).

Le Titulaire s'assure de la bonne utilisation des comptes utilisateurs qui lui ont été fournis, et s'engage notamment à strictement respecter les obligations suivantes :

- garantir que les codes d'accès ne sont accessibles qu'aux personnels autorisés ;
- traiter les informations de connexion comme étant hautement confidentielles ;
- utiliser les ressources du Mipih conformément à leur destination (dans la stricte limite de la prestation objet du marché) ;
- ne pas altérer ou détruire des traces ou preuves relatives à des actions ou des événements sur les Systèmes d'information du Mipih, que ces éléments concernent le Titulaire ou non ;
- ne pas entraver le fonctionnement des équipements opérationnels et ceux de sécurité et en aucun cas porter atteinte à la production informatique du Mipih ;
- avertir les Responsables de la Sécurité de l'Information (RSSI) de tout dysfonctionnement constaté et/ou de toute anomalie (générée de son fait ou ne le concernant pas mais relevant de la sécurité) observée lors de l'exécution de ses prestations. La procédure d'alerte consiste à prévenir par tout moyen et sans délai les RSSIs.

Le Titulaire est informé que tout accès au SI du Mipih est tracé, conformément aux lois informatiques et Liberté. Les traces sont archivées pour une durée d'un an.

7.8 Signalements de sécurité

Pour les prestations, produits et services qu'ils fournissent dans le cadre du marché, le titulaire, au titre de son devoir permanent de conseil et d'information, signale sans délai tout événement pouvant affecter la disponibilité, l'intégrité, la pérennité, la confidentialité ou la perte d'informations du Mipih qu'il détient, auxquelles il accède ou qu'il manipule.

Le titulaire doit effectuer une veille sur les vulnérabilités techniques de ses composants, informer le Mipih dans les plus brefs délais de l'existence d'une vulnérabilité, de son niveau de criticité et des conséquences potentielles, mettre en œuvre les moyens nécessaires pour corriger la vulnérabilité ;

Réciproquement, les outils numériques mis à disposition permettent aux bénéficiaires et leurs experts en cybersécurité de signaler directement au titulaire de possibles failles ou détournements de dispositifs de sécurité.

Après analyse partagée et vérification, le titulaire a obligation d'enregistrer les failles auprès des autorités compétentes (CERT nationaux pour les éditeurs, registres RGPD et CNIL ou équivalent pour la divulgation de données personnelles,

ANSSI pour les opérateurs d'importance vitale ou de services essentiels, cybersécurité.santé.gouv.fr pour les dispositifs de santé, etc.) en suivant les réglementations établies.

7.9 Dispositifs connectés au Système d'Information

Dans le cas où l'exécution des prestations objet du marché nécessiterait la connexion de dispositifs au SI du Mipih, le Titulaire s'engage à strictement respecter les dispositions listées ci-dessous, que le dispositif soit rétrocédé au Mipih ou qu'il soit propriété du Titulaire :

- ne connecter aucun matériel informatique sans l'accord explicite et écrit du Responsable de l'infrastructure du Mipih ;
- tous les supports d'information amovibles (support USB, disque Dur amovible, ...) devront avoir été balayés en présence d'un agent du Mipih par un antivirus à jour, et ce à chaque fois qu'ils doivent être utilisés, sur les matériels du Mipih. Le Titulaire s'engage par ailleurs à suivre le même mode opératoire pour l'utilisation de tels supports sur son propre matériel ;
- signaler les failles de sécurité des applicatifs fournis ;
 - respecter l'ensemble des règles de sécurité définies dans le CCTP ou cahier des charges du marché et à défaut les bonnes pratiques concernant : la gestion de configuration ;
 - la gestion de la sécurité physique ;
 - la gestion de l'exploitation et des communications (vérification du bon fonctionnement, mises à jour, protection contre les codes malveillants, sécurité des réseaux, sécurité des données, gestion des supports amovibles, surveillance, journalisation, sauvegardes, règles de destruction de données lors du transfert de matériels informatiques ;
 - la maîtrise des accès (contrôle d'accès au réseau, authentification des utilisateurs, droits d'accès) ;
 - la maîtrise de la conformité ;
- respecter les bonnes pratiques de développement logiciel :
 - progiciels de type « application ou service web » : respect du guide pratique PGSSI-S « Règles pour la mise en place d'un accès web au SIS pour des tiers » ;
 - OWSAP, ANSSI ;
 - Autres progiciels ;
- Fournir une fonctionnalité de récupération par le Mipih des données conservées par l'équipement connecté pour le réutiliser dans un dispositif différent en fin de marché.

Dans tous les cas, un titulaire de marché est tenu de fournir à première demande la documentation nécessaire à la sécurisation de leurs fournitures dans les systèmes d'information, la protection des données des bénéficiaires et aux démonstrations du respect de leurs obligations par les bénéficiaires du marché. En particulier, la documentation explicitant tous les flux échangés (entrants et sortants, applicatif mais aussi de maintenance, de statistiques, de mise à jour, d'administration distante, etc), et les dispositifs de contrôle d'accès et de maintien en condition de sécurité.

Si l'emploi sécurisé du produit ou du service nécessite des actions particulières de la part des bénéficiaires du marché, elles doivent être clairement identifiées dans un chapitre Sécurité du mode d'emploi (par exemple, la procédure de changement des mots de passe par défaut ou des interfaces exposées, de mise à jour de composants logiciels...).

7.9.1 Maintien en condition de sécurité

La politique de sécurité exige la mise à jour des composants logiciels vers des versions supportées par l'éditeur ou la communauté Open Source qui les produisent. Dans ces conditions, une vérification d'aptitude au bon fonctionnement ou au service régulier (VABF et VSR) est refusée si des composants ne sont pas à jours des correctifs de failles de sécurité.

La responsabilité du maintien en condition de sécurité d'un titulaire comprend les composants et services développés en propre mais aussi ses composants et dépendances amont ou sous-traités.

Un candidat ou titulaire ne peut conditionner ses garanties de bon fonctionnement de fournitures ou prestations qu'il fournit à l'emploi de composants dans une version non supportée, sauf à démontrer une contrainte supérieure et proposer à ses frais des moyens de cantonner les risques, ou démontrer que les risques sont négligeables dans le contexte d'emploi.

Dans tous les cas, les unités d'œuvre portant le maintien en condition opérationnelle (labellisée MCO mais aussi tierce maintenance applicative (TMA) ou simplement hébergement incluent le maintien en condition de sécurité et donc la mise en œuvre des correctifs de failles de sécurité.

7.10 Interventions à distance

Les interventions à distance (télésurveillance, télémaintenance, téléassistance) sont nécessaires au bon maintien en condition opérationnelle de certains équipements utilisés par le Mipih.

Dans l'hypothèse où le Titulaire serait amené à intervenir à distance dans le cadre de l'exécution des prestations objet du marché, la traçabilité des accès et des actions est assurée par un « bastion » authentifiant qui enregistre les actions imputables au titulaire du compte. Celui-ci s'engage à strictement respecter les consignes suivantes :

- s'assurer de la mise à jour régulière des personnels autorisés, notamment suite à des départs éventuels de personnels, fin d'intervention d'un sous-traitant Les accès adéquats devront être révoqués en cas de cessation du besoin et/ou départ du personnel concerné ;
- obtenir l'accord préalable du Mipih avant chaque opération de télémaintenance dont il prendrait l'initiative. Il est précisé que les accès à la production sont strictement interdits, tout comme aux environnements d'intégration, sauf accord préalable exprès de la part du responsable de l'infrastructure ;
- prendre toute disposition permettant au Mipih d'identifier la provenance de chaque intervention extérieure ;
- transmettre systématiquement au responsable du projet ou de l'application 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, application, middleware, réseau) ;

- s'assurer de l'intégrité de l'équipement utilisé pour l'intervention, de la mise de celui-ci par rapport aux derniers correctifs de sécurité et protection contre les codes malveillants (antivirus, antimalware ...) ;
- assurer de façon générale la protection contre tout accès non autorisé par tous les moyens adéquats (protection périmétrique, protection physique ...) ;
- ne pas se connecter simultanément à des sources potentiellement compromettantes telles qu'Internet, autres réseaux d'accès distant, ... ;
- respecter l'ensemble des règles décrites dans le corpus documentaire de la PGSSI-S de l'ASIP Santé pour les interventions à distance sur les Systèmes d'Information de Santé (v1.0) et en particulier mettre en œuvre les éléments de sécurité suivants :
 - l'intervention est encadrée par un règlement ;
 - le Titulaire est tenu d'effectuer toutes les activités de la prestation au sein de l'Union Européenne ou de se conformer aux règles définies par la CNIL pour les prestations hors zone de l'UE. S'il n'est pas possible de situer ou connaître la localisation des activités (personnel et serveurs informatiques), le Titulaire ne pourra exécuter les prestations et pourra être sanctionné au titre du marché ;
 - le Titulaire est tenu de signaler sans délai tout changement relatif à sa situation administrative (rachat, fusion, liquidation ...) ;
 - assurer la sécurité de sa plateforme d'intervention à distance, tant d'un point de vue accessibilité que protection des données et des logiciels ;
 - restreindre les accès logiques des postes d'intervention aux seules personnes autorisées ;
 - être en mesure de déterminer en toute circonstance l'identité de toute personne qui se connecte ou s'est connecté sur la plateforme et en assurer la traçabilité ;
 - mettre en œuvre des moyens et des procédures conformes aux règles de l'art pour lutter contre les incidents pouvant affecter la sécurité du SI, de ses informations ou la sécurité de l'intervention elle-même ;
 - établir un Plan d'Assurance Sécurité (PAS) qui décrit les dispositions de sécurité que le Titulaire met en œuvre pour exécuter ses prestations (ou fait référence à une documentation consultable par les responsables du SI) ;
 - définir avec les responsables du SI les modalités pratiques permettant la bonne réalisation de l'intervention à distance.

Dans le cas de l'attribution d'un compte utilisateur générique (affecté au Titulaire et non nominativement à un de ses préposés), le Titulaire gère la traçabilité des accès. Sur simple demande ; le Mipih doit disposer sans délai de l'historique nominatif de cet accès générique (utilisateur de l'accès générique, dates et heures de connexion, durée de connexion et pour quelles actions).

7.11 Règles spécifiques à l'hébergement

7.11.1 Hébergement au Mipih

Le Titulaire s'engage à respecter et à faire respecter par ses préposés les exigences de la PSSI-MCAS relatives aux principes d'architecture de la zone d'hébergement :

- l'architecture de l'infrastructure des centres informatiques est conçue de façon à satisfaire l'ensemble des besoins en disponibilité, confidentialité, traçabilité et intégrité ;
- le principe de défense en profondeur doit être respecté, en particulier par la mise en œuvre successive de « zones démilitarisées » (DMZ), d'environnement de sécurité en zone d'hébergement, de machines virtuelles ou physiques dédiées, de réseaux locaux virtuels (VLAN) appropriés, d'un filtrage strict des flux applicatifs et d'administration.

Le titulaire prend l'engagement de respecter les exigences de sécurité préalable à l'hébergement au Mipih et les règles de PGSSI-S décrites dans le CCTP. Le candidat ou titulaire doivent apporter leur concours en matière de documentations et de réponses aux questions, permettant d'analyser les risques résiduels en matière de confidentialité, authentification, traçabilité, intégrité, disponibilité et résilience.

Complément pour l'Hébergement de données de santé :

L'accès par les utilisateurs du Titulaire aux services et informations du SI-DonnéesSanté doit être strictement limité au périmètre des missions confiées dans le cadre du marché.

A ce titre, le Titulaire s'interdit :

- d'accéder ou transmettre des données de santé à caractère personnel, sauf pour des raisons techniques justifiées. En ce cas, les accès doivent être tracés. Les transferts de ces données doivent être rendus confidentiels par un moyen de cryptage ;
- d'accéder à des données détenues par des utilisateurs extérieurs à ses services, quand bien même ces données n'auraient pas expressément été protégées.

7.11.2 Hébergement hors Mipih

Le titulaire devra apporter toutes les preuves de la sécurité du site d'hébergement de la solution et du respect des droits des personnes. Il s'agit en particulier du respect des textes et des règlements en vigueur relatifs à l'hébergement (certifications HDS, 27001, RGS, RGPD,....cf. Article 4. Règlementation en vigueur).

A première demande, le candidat ou titulaire identifie tous les prestataires techniques hébergeant ou stockant les données et leurs copies, utilisées ou échangées en cours de marché ainsi que leur localisation.

7.12 Destruction des données

Dans le cadre de la destruction des données, le Titulaire s'engage à respecter scrupuleusement les exigences de sécurité formulées par la PSSI, à savoir le respect du guide pratique « destruction de données lors du transfert de matériels

informatiques des Systèmes d'Information de Santé (SIS) du corpus documentaire PGSSI-S de l'ASIP Santé.

7.13 Développements réalisés par le Titulaire

Si le Titulaire est amené à exécuter des prestations de développement dans le cadre de l'exécution du marché, il s'engage à :

- former ses développeurs sur le développement sécurisé et sur les vulnérabilités classiques ;
- utiliser des outils permettant de minimiser les erreurs introduites durant le développement (outils d'analyse statique de code, utilisation de bibliothèques réputées pour leur sécurité, ...) ;
- produire la documentation technique décrivant l'implantation des protections développées (gestion de l'authentification, stockage des mots de passe, gestion des droits, chiffrement ...) ;
- respecter les normes de développement sécurisé, qu'elles soient propres au développeur, publiques (ex : OWASP, ANSSI) ou propres au commanditaire ;
- corriger, dans un temps raisonnable, les vulnérabilités introduites durant le développement et qui lui sont remontées, en incluant automatiquement les corrections des autres occurrences des mêmes erreurs de programmation ;
- permettre au Mipih de réaliser ou faire réaliser par un prestataire désigné par lui un audit de la qualité du code pendant le développement.

7.14 Protection des données de test

Le Titulaire du marché s'engage à respecter le fait que les données utilisées comme jeux d'essais pour les applicatifs ne peuvent être des données réelles nominatives, ni des données de santé à caractère personnel. Les données servant aux tests doivent obligatoirement être rendues anonymes.

Dans l'hypothèse où des données réelles s'avèreraient nécessaires, le Titulaire s'engage à prendre des mesures spécifiques de protection devant garantir la confidentialité et la non divulgation. En pareille circonstance, le Titulaire :

- sollicite un accord formel de la part du Mipih ;
- procède à l'identification nominatives de son personnel pouvant accéder à ces données ;
- utilise ces données dans un environnement cloisonné.

Article 8. Audits, traçabilité et contrôle

Le Mipih se réserve la possibilité d'effectuer ou de faire effectuer des contrôles des dispositions de sécurité prises par le Titulaire dans le cadre de l'exécution des prestations. A ce titre, le Titulaire s'engage à fournir au Mipih, ou à toute personne qu'il aura mandatée, l'ensemble des éléments nécessaires aux vérifications (obligation de collaboration).

Les différents contrôles et mesures, matérialisés notamment par des constats ou des rapports effectués par la Personne Publique ou par un tiers à sa demande, sont opposables au Titulaire.

Par ailleurs, au titre de son devoir permanent de conseil et d'information, le Titulaire informe le Mipih sans délai de tout évènement pouvant affecter la disponibilité, l'intégrité, la traçabilité, la confidentialité ou la perte d'informations du Mipih qu'il détient, auxquelles il accède ou qu'il manipule.

Article 9. Responsabilité

Le Titulaire est responsable de tous les dommages corporels, matériels et immatériels, direct ou indirects, trouvant leur origine aussi bien dans une exécution fautive (même partielle), mauvaise exécution ou inexécution des obligations visées par la présente charte.

Le Titulaire est seul responsable de l'action de ses personnels et des personnels intervenant pour son compte (sous-traitant ...).

Nonobstant les actions en responsabilité contractuelle susceptibles d'être engagées par le Mipih, des actions civiles (atteinte au droit à l'image d'un tiers ...) et/ou pénales (intrusion frauduleuse dans le SI, violation du secret professionnel ...) pourront être ouvertes.

ANNEXE 1. Engagement de confidentialité

Toute personne intervenant au titre de l'exécution du marché intervenant sur site ou à distance dans des opérations liées au SI du Mipih doit au préalable s'engager sur la confidentialité selon les termes ci-après.

Le Titulaire tient et gère un état nominatif des personnes autorisées à intervenir au titre de l'exécution du marché et communique sans délai cet état au Mipih sur simple demande. L'engagement de confidentialité signé individuellement par chaque intervenant désigné est adossé à l'état nominatif et communiqué au Mipih préalablement à toute intervention (obligation de résultats).

ENGAGEMENT DE CONFIDENTIALITE NOMINATIF

Je soussigné, M. Mme, intervenant en qualité de pour le compte de la société dont je suis salarié, m'engage à :

- utiliser les ressources du Mipih uniquement dans le cadre du projet de la prestation ;
- ne pas divulguer mon compte d'accès au système d'information ;
- respecter la Charte des bons usages du Système d'Information du Mipih ;
- ne pas divulguer d'informations sur le Mipih et le contenu de ma prestation à un tiers, pendant et après ma mission ;
- à rendre au Mipih l'ensemble des informations et supports à la fin de la mission ;
- accéder uniquement aux informations du Mipih nécessaires au projet ;
- accéder aux locaux du Mipih uniquement dans les horaires, jours et périmètre convenus dans le contrat et nécessaire à ma mission ;
- ne pas essayer de m'introduire dans des salles non autorisées ou avec d'autres moyens que ceux mis à ma disposition ;
- ne pas accéder aux salles machines et salles techniques (informatiques et télécommunications) du Mipih, sauf autorisation écrite spéciale ou accompagné d'un agent du Mipih et si l'objet de la prestation le justifie ;
- ne pas permettre l'accès aux personnes non autorisées par le Mipih dans les locaux du Mipih ;
- respecter les systèmes de sécurité physique mis en place à le Mipih, en particulier fermer systématiquement à clé si je le peux, les portes derrière moi, même en cas d'absence de courte durée ;
- assurer la protection physique du matériel mis à ma disposition ;
- ne réaliser aucune copie ou duplicata des moyens d'accès mis à ma disposition ;
- ne pas entraver le fonctionnement des équipements opérationnels et ceux de sécurité.

A, Le

Nom prénom

Cachet de l'entreprise et signature