Guide des clauses de sécurité des systèmes d'information types à intégrer dans les marchés publics

Juillet 2019

L'Agence nationale de sécurité des systèmes d'information (ANSSI) et la Direction des achats de l'Etat (DAE) ont piloté un groupe de travail interministériel réunissant les experts de la sécurité informatique afin de recueillir leurs expériences et d'établir un guide destiné à aider les services de l'Etat à prendre en compte la dimension SSI dans la préparation de leurs marchés publics.

Les travaux du groupe de travail ont abouti à la réalisation d'un guide de clauses génériques. Ce dernier a fait l'objet d'une validation par le bureau des affaires juridiques de la DAE avant d'être soumis à commentaires publics sur la plateforme de la Direction interministérielle du numérique et des systèmes d'information et de communication (DINSIC) en juillet 2019.

Ce guide a pour objectif de fournir aux acheteurs, rédacteurs, juristes, prescripteurs (profil métier ou technique), une méthode de travail et des exemples de clauses relatives à la sécurité des systèmes d'information à intégrer lors de la préparation de marchés publics.

Guide des clauses de sécurité des systèmes d'information types à intégrer dans les marchés publics

Table des matières

GLOSSAIRE

ACHETEUR PUBLIC
Définition basée sur le répertoire interministériel des métiers de l'Etat (RIME)
Personne qui définit et met en œuvre des stratégies achat de toute nature en vue de satisfaire les besoins qualitatifs et quantitatifs des services et de contribuer à la performance des achats dans le respect des règles de la commande publique.
L'acheteur public est chargé de piloter les projets achat et de suivre leur exécution, de mesurer la performance achat, de mener la veille économique, notamment en analysant les marchés fournisseurs. Il cherche à promouvoir les marchés disponibles auprès des utilisateurs et mesure leur degré de satisfaction.
Il coordonne, en liaison avec les prescripteurs et les approvisionneurs-achat, la définition du juste besoin. Lorsqu'il est chargé de porter la procédure juridique de contractualisation, il rédige les éléments du dossier de consultation relatifs à l'expression du besoin et du choix du fournisseur, analyse les offres, négocie (lorsque cela est permis par la réglementation) et sélectionne les offres attributaires.

ATTRIBUTAIRE
L'attributaire d'un marché public est le soumissionnaire classé premier à l'issue de l'analyse des offres auquel il est envisagé d'attribuer le marché.

ACTE D'ENGAGEMENT (AE)
Document contractuel, signé des deux parties qui constitue la pièce principale du marché.

CAHIER DES CHARGES
Document contractuel qui décrit le besoin de l'acheteur, exprimé sous forme de spécifications techniques et /ou d'exigences fonctionnelles. Il détermine également les conditions dans lesquelles les prestations qui font l'objet du marché doivent être exécutées.

CAHIER DES CLAUSES ADMINISTRATIVES GÉNÉRALES (CCAG)
Arrêté ministériel auquel l'acheteur peut faire référence dans les documents de la consultation, auquel cas il devient un document contractuel. L'acheteur a toujours la possibilité d'y déroger de manière expresse au sein des autres pièces contractuelles. Il contient des stipulations d'ordre administratif et financier applicables à un même secteur d'activité. Il existe cinq CCAG en fonction de l'objet du marché : Travaux - Marchés industriels - Prestations intellectuelles - Fournitures courantes et prestations de services - Techniques de l'information et de la communication.

CAHIER DES CLAUSES ADMINISTRATIVES PARTICULIÈRES (CCAP)
Document contractuel qui décrit les conditions administratives particulières d'exécution des marchés, notamment les conditions administratives et financières (avances, acomptes, conditions de livraison, pénalités…).

CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES (CCTP)
Document contractuel qui décrit les conditions techniques particulières d'exécution des marchés, sous forme d'exigences minimales (approche fonctionnelle) ou de spécifications fonctionnelles techniques.

CADRE DE RÉPONSE
Document que l'acheteur peut inclure aux documents de la consultation et visant à faciliter l'analyse des offres.

CANDIDAT
Personne physique ou morale publique ou privée qui présente sa candidature dans le cadre d'une procédure de marché public. Dans ce présent guide, la notion de candidat renvoie indifféremment aux notions de candidat au sens strict, mais aussi de soumissionnaire, d'opérateur économique ou d'entreprise.

CANDIDATURE
Document déposé par un candidat à une procédure de marché public relatif notamment à ses aptitudes et capacités pour exécuter le marché public.

DOCUMENTS DE LA CONSULTATION (DC)
L'ensemble des documents fournis par l'acheteur ou auxquels il se réfère afin de définir ses besoins et de décrire les modalités de la procédure de passation, y compris l'avis d'appel à la concurrence. Les informations fournies sont suffisamment précises pour permettre aux opérateurs économiques de déterminer la nature et l'étendue du besoin et de décider de participer à la procédure.

OPÉRATEUR ÉCONOMIQUE
Terme générique qui couvre à la fois les notions d'entrepreneur, fournisseur et prestataire de services. Il désigne toute personne physique ou morale, publique ou privée, ou groupement de ces personnes qui propose une offre dans le cadre d'un marché public pour la réalisation de travaux et/ou d'ouvrages, la fourniture de produits ou de services. Dans ce guide, la notion d'opérateur économique est remplacée par le terme générique de candidat.

PRESCRIPTEUR
Personne qui définit techniquement les besoins objet du marché, pour son compte ou celui d'autres personnes. Il est souvent placé dans une direction métier.

RÈGLEMENT DE LA CONSULTATION (RC)
Document non contractuel figurant dans les documents de la consultation. Il précise les modalités de la mise en concurrence, les critères d'attribution des offres et leur pondération ainsi que la possibilité d'une négociation. Il complète l'avis d'appel à la concurrence.

SOUS-TRAITANCE
Opération par laquelle le titulaire confie, sous sa responsabilité et sous son contrôle, à une autre personne physique ou morale appelée sous-traitant l'exécution d'une partie des tâches qui sont à sa charge dans le cadre du marché public qui lui a été attribué. Le titulaire demeure, face à la personne publique, le seul responsable de l'exécution des prestations.

TITULAIRE
L'attributaire d'un marché public devient le titulaire de ce marché après qu'il ait apporté la preuve de la régularité de sa situation et suite à la signature du marché et sa notification par l'acheteur.

SOUMISSIONNAIRE
Opérateur économique qui présente une offre dans le cadre d'une procédure de marché public. Dans présent guide le vocable utilisé pour désigner le soumissionnaire est « le candidat ».

Introduction

Contexte et périmètre

Ce guide a pour objectif de fournir aux acheteurs, rédacteurs, juristes, prescripteurs (métiers ou techniques), une méthode de travail et des clauses types de sécurité des systèmes d'information à intégrer lors de la préparation de marchés publics.

Il doit être utilisé pour la préparation de tous les marchés pour lesquels tout ou partie des produits ou services achetés font appel, directement ou indirectement, à des dispositifs informatiques.

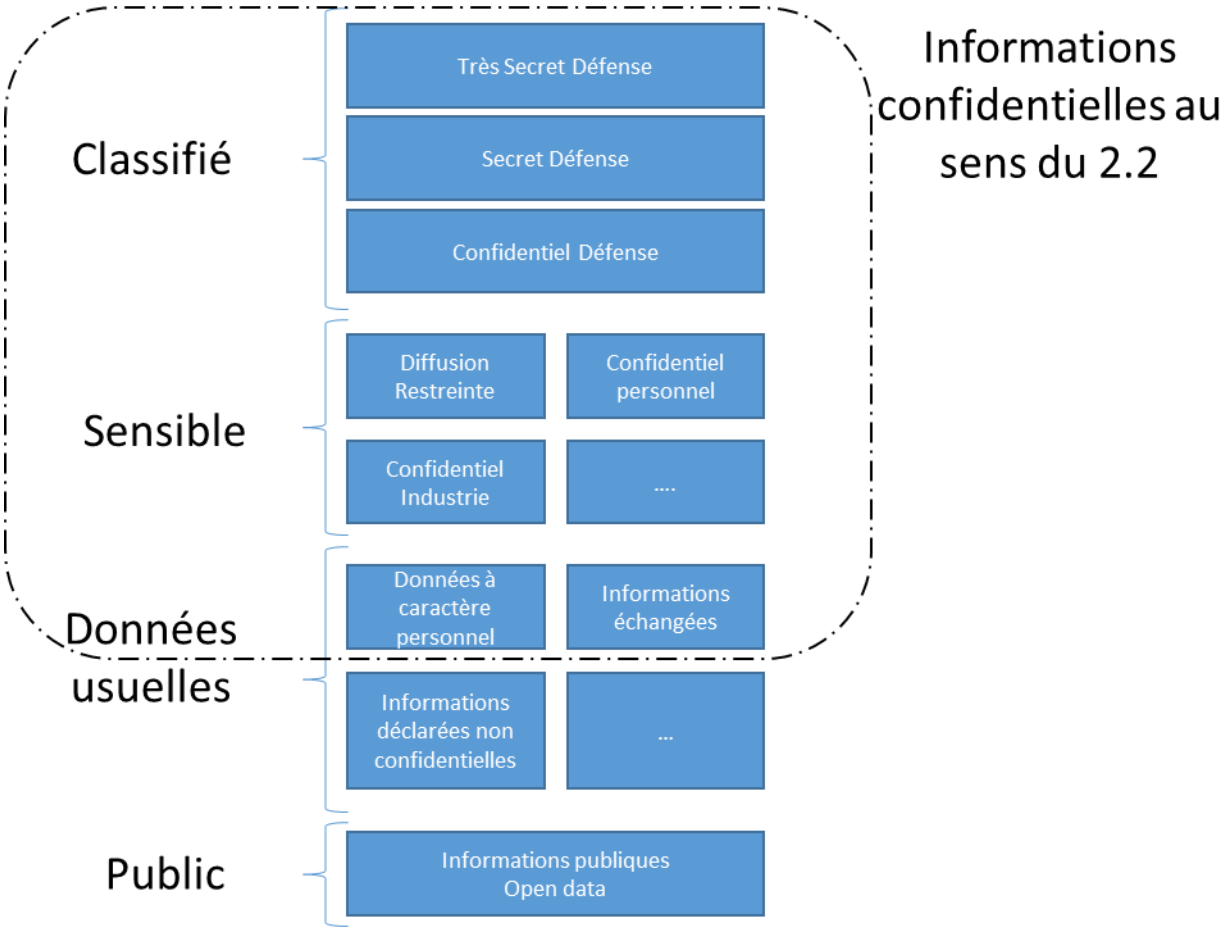
Son utilisation assure un niveau de protection suffisant pour la plupart des marchés. Les acheteurs sont invités à mener une analyse de risques[1] pour préciser leur besoin et choisir les clauses les plus pertinentes. Dans certains cas, notamment des achats de produits et services traitant des informations sensibles[2], les clauses proposées dans ce document devront être complétées et renforcées par un travail commun entre les acheteurs et le responsable de la sécurité des systèmes d'information (RSSI).

Lorsque l'objet ou les livrables du marché relèvent d'une réglementation pouvant avoir des conséquences aussi bien pour le titulaire que pour l'acheteur (notamment protection du secret de défense, protection des infrastructures vitales), les acheteurs sont invités, en amont de la procédure de passation, à se rapprocher de la chaîne fonctionnelle de la sécurité des systèmes d'information à travers, par exemple, leur officier de sécurité des systèmes d'information et à mentionner ces réglementations dans les documents de la consultation.

Le guide a été structuré autour de l'organisation et des normes internes s'appliquant aux services de l'Etat, il a été produit par la DAE avec l'appui de l'ANSSI et en concertation avec les ministères. Son contenu, le cas échéant, doit être adapté en fonction des normes internes régissant d'autres entités publiques.

1 Par exemple avec la méthode EBIOS développée par l'ANSSI : https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/ ou https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/.

2 Au sens de l'instruction interministérielle n°901 relative aux mesures de protection des systèmes d'information traitant d'informations sensibles non-classifiées de défense de niveau Diffusion Restreinte (DR), informations dont la divulgation à des personnes non autorisées, l'altération ou l'indisponibilité sont de nature à porter atteinte à la réalisation des objectifs des acheteurs qui les détiennent.


Classifié
Très Secret Défense
Secret Défense
Confidentiel Défense
Informations confidentielles au sens du 2.2
Sensible
Diffusion Restreinte
Confidentiel personnel
Confidentiel Industrie
....
Données usuelles
Données à caractère personnel
Informations échangées
Informations déclarées non confidentielles
...
Public
Informations publiques
Open data

Objet du document

Le présent guide présente un ensemble de recommandations ainsi que des clauses types à insérer dans les documents de la consultation liées à la sécurité du système d'information, en particulier les marchés concernant les prestations intellectuelles, l'hébergement externe, l'achat de matériels et logiciels, l'exploitation et la supervision ou les études et le développement.

Le guide distingue :
- les clauses relatives à la passation à intégrer dans le règlement de la consultation (RC) ;
- les clauses relatives à l'exécution à intégrer dans le cahier des clauses administratives particulières (CCAP) et le cahier des clauses techniques particulières (CCTP).

Il appartient à l'acheteur de vérifier la bonne adéquation des clauses avec les spécificités de son marché et, le cas échéant, de les adapter notamment quand des réglementations spécifiques trouvent à s'appliquer.

Les exemples de clauses types à intégrer dans les documents du marché sont matérialisés par un encadré gris.

1. Clauses à intégrer dans le règlement de la consultation (RC)

1.1. Le plan d'Assurance Sécurité (PAS)

En principe, les clauses de Sécurité figurent au CCAP et/ou CCTP. Par exception et lorsque que les clauses de sécurité nécessitent des justifications spécifiques sur les moyens que le titulaire met en œuvre pour s'y conformer, il peut être demandé aux opérateurs économiques au moment de la consultation un Plan d'Assurance Sécurité (PAS). Ce dernier est demandé dans les marchés informatiques, de type infogérance par exemple.

Le PAS décrit l'ensemble des actions spécifiques que le candidat doit mettre en œuvre lors de l'exécution du marché pour garantir le respect des exigences de sécurité de l'acheteur.

Le PAS[3] se présente sous la forme d'un cadre de réponse : il offre une structure pour la réponse des soumissionnaires aux exigences de sécurité, ce qui permet de mieux évaluer la pertinence de la couverture des exigences. Il facilite également la comparaison entre les différentes offres.

Les acheteurs peuvent proposer dans le PAS un tableau vierge répertoriant toutes les exigences de sécurité sur lesquelles ils attendent un positionnement des soumissionnaires. Ces derniers doivent lister la ou les mesures de sécurité techniques, procédurales et organisationnelles qu'ils retiennent pour répondre à chaque exigence définie par l'acheteur dans le CCAP et le CCTP.

CLAUSE TYPE :

Document : RC

ARTICLE X.X « Contenu des documents de la consultation »

Les documents de la consultation sont les suivants :

☐ *[le présent règlement de la consultation]*
☐ *[les annexes au règlement de la consultation]*
(…)
☐ *[le cahier des clauses administratives particulières]*
☐ *[le cahier des clauses techniques particulières]*
☐ *[le cadre de réponse dont le plan-type d'assurance-sécurité (PAS)]*
☐ *[le cadre de réponse dont le plan de prévention des risques (PPR)]*

[3] Plus d'informations sur le PAS et un plan type sont présents dans le guide sur l'infogérance à partir de la page 24 : https://www.ssi.gouv.fr/guide/externalisation-et-securite-des-systemes-dinformation-un-guide-pour-maitriser-les-risques/

ARTCLE X.X: « présentation de l'offre »
L'offre du soumissionnaire comporte les pièces suivantes :
☐ *[le mémoire technique répondant au cahier des charges]*
☐ *[le bordereau des prix unitaires (BPU)]*
☐ *[la décomposition du prix global et forfaitaire (DPGF)]*
☐ *[le détail quantitatif et estimatif (DQE)]*
(…)
☐ *[le plan –type d'assurance-sécurité (PAS)]*
☐ *[le plan de prévention des risques (PPR)]*
☐ *[le cas échéant, le formulaire d'engagement et de reconnaissance de responsabilité]*

Le Plan d'Assurance Sécurité est remis par chacun des soumissionnaires avec son offre. Les offres sont classées par ordre décroissant en appliquant les critères d'attribution préalablement choisis et portés à la connaissance des candidats.

1.2. Formulaire d'engagement de reconnaissance de responsabilité

Le titulaire pressenti confirme avoir pris connaissance des règles de sécurité à appliquer en signant le *formulaire d'engagement et de reconnaissance de responsabilité* (document disponible en annexe du présent guide).

Ce document doit figurer, le cas échéant, dans la liste des documents contractuels visés dans le CCAP. Cf. point 2.1.4 pour la clause.

1.3. Sous-traitants

En matière de marchés publics, la sous-traitance est l'opération par laquelle le titulaire d'un marché confie à un opérateur tiers l'exécution d'une partie des prestations qui lui ont été confiées par l'acheteur[4].

Les obligations du titulaire**, y compris les clauses de sécurité,** s'appliquent intégralement à ses sous-traitants et sous sa responsabilité.

En application des CCAG, le titulaire doit informer ses sous-traitants des obligations de confidentialité et des mesures de sécurité qui s'imposent à lui pour l'exécution du marché et doit s'assurer du respect de ces obligations par ses sous-traitants.

Toutefois[5], l'acheteur peut exiger que certaines tâches du marché, comme celles relatives à la sécurité des systèmes d'information, soient effectuées directement par le titulaire et non par

[4] Le régime juridique relatif à la sous-traitance est défini par la loi n° 75-1134 du 31 décembre 1975 et, pour les règles propres aux marchés publics passés par des acheteurs soumis au code de la commande publique, par les articles L. 2193-1 à L. 2193-14 ainsi que les articles R. 2193-1 à R. 2193-22 du code (marchés publics classique) et R. 2393-24 à R. 2393-40 du code (marchés publics de défense ou de sécurité).

[5] Cf. article L. 2193-3 du code (marchés publics classiques) et L. 2393-7 du code (marchés publics de défense ou de sécurité)

un sous-traitant : l'acheteur peut restreindre le recours à la sous-traitance en exigeant que certaines tâches essentielles soient effectuées directement par le titulaire. **Cette possibilité de limiter la sous-traitance suppose, au regard du principe de transparence des procédures, que l'acheteur ait clairement indiqué dans l'avis d'appel à la concurrence ou le règlement de la consultation, les tâches essentielles concernées.**

Document : RC

ARTICLE X.X « Précisions concernant la sous-traitance »
ARTICLE X.X.X « Tâches essentielles »

○*[Les tâches essentielles suivantes doivent être exécutées par le titulaire et ne peuvent faire l'objet de sous-traitance : (A COMPLETER).]*

○*[L'acheteur n'exige pas que certaines tâches essentielles soient effectuées directement par le titulaire.]*

1.4. Hébergement des données et des services

En fonction de la sensibilité des données ou des services qui seront confiés au titulaire, l'acheteur peut demander au candidat des précisions sur la localisation et l'hébergement des données ou des services liés à la prestation :

Document : RC

ARTICLE X.X « Information sur la localisation géographique des données et des services »

- Le soumissionnaire précise dans son offre les lieux géographiques dans lesquels :
  - Les données informatiques liées à la prestation seront hébergées ;
  - Les services objets de la prestation seront localisés ;
  - Les systèmes d'accès et d'administration des services liés à la prestation seront localisés.

De même, le soumissionnaire précise dans son offre si ses infrastructures (techniques ou organisationnelles) sont gérées ou simplement accessibles par une entité juridique appartenant à un pays disposant de lois autorisant ce pays à accéder aux données.

- Respect des normes de sécurité environnementales : le soumissionnaire décrit le cas échéant les risques environnementaux dont font l'objet les sites

hébergeant les données ou du service et précise dans un plan de prévention des risques (PPR) les mesures mises en œuvre pour couvrir ces risques.

2. Clauses à intégrer dans le CCAP

Les marchés peuvent faire référence à d'autres CCAG que le CCAG-TIC. Le guide couvre en effet tous les marchés et pas uniquement les marchés TIC : il peut s'agir par exemple de marchés de prestations de livraison comportant l'accès au portail internet du titulaire.
Le CCAG choisi dépend de l'objet du marché public. Dans un souci de simplicité, il sera fait référence au CCAG-TIC dans ce guide. L'acheteur doit adapter les clauses types en fonction du CCAG choisi

Dans son article 5, le CCAG-TIC énonce un certain nombre de clauses principales liées à la sécurité et à la confidentialité[6]. Les clauses du CCAP peuvent compléter ce corpus afin d'être plus précisément adaptées au cas du marché public. Pour les clauses relatives à la sécurité informatique, il est nécessaire de compléter le CCAG-TIC qui ne prévoit que des mesures de sécurité physique des zones protégées.

2.1. Pièces contractuelles du marché

Dans le cas des marchés relatifs aux technologies de l'information et de la communication (TIC), le CCAG-TIC est le plus souvent retenu comme cadre de clauses générales[7].

Cf. 2.1.4 pour la clause.

2.1.1. Plan d'assurance sécurité (PAS)

Si l'acheteur a exigé la remise d'un PAS lors de la consultation, le CCAP doit lister ce PAS parmi les pièces contractuelles du marché en complément de l'article 4 du CCAG-TIC.

Cf. 2.1.4 pour la clause.

2.1.2. Politique de sécurité du Système d'Information (PSSI) de l'acheteur

L'obligation de respecter la Politique de Sécurité du Système d'Information (PSSI) de l'acheteur doit être indiquée dans le CCAP et figurer dans la liste des documents contractuels.

Cf. point 2.1.4 pour la clause.

6 Extrait du CCAP du marché interministériel de conseil, d'expertise et d'audit en Sécurité des Systèmes d'Information
7 Cf. Arrêté du 16 septembre 2009 portant approbation du cahier des clauses administratives générales applicables aux marchés publics de techniques de l'information et de la communication.

2.1.3. Réglementations spécifiques et autres documents contractuels

L'annexe n°1 de ce guide mentionne une liste de documents que l'acheteur peut rendre contractuels en fonction de ses besoins. Pour ce faire, il devra compléter la clause ci-dessus listant les documents contractuels applicables au marché.

C'est le cas si des réglementations spécifiques doivent s'appliquer au marché.

Exemples :

- Données classifiées :
  - l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale
- Réglementations spécifiques à la protection de certains systèmes d'information :
  - l'instruction interministérielle n°901/SGDSN/ANSSI du 28 janvier 2015 relative aux mesures de protection des systèmes d'information traitant d'informations sensibles non-classifiées de défense de niveau Diffusion Restreinte (DR)
  - le référentiel général de sécurité (RGS) dans sa version en vigueur
  - les articles L. 1332-6-1 et L. 1332-6-3 du code de la défense qui peuvent imposer l'utilisation de produits et de services (audit, détection) qualifiés ;

- Données à caractère médical : article L. 1111-8 du code de la santé publique sur l'hébergement des données de santé ;
- Données de recherche, données stratégiques et techniques : décret n° 2011-1425 du 2 novembre 2011 portant application de l'article 413-7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation, arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation
- Données à caractère personnel : règlement (UE) 2016/679 du parlement européen et et conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) dit RGPD

L'acheteur peut s'appuyer sur les guides de l'ANSSI pour définir ses exigences (voir l'annexe 1 de ce guide). Les guides d'hygiène informatique[8], de bonnes pratiques[9] et celui sur l'administration sécurisée[10] constituent un socle fortement recommandé par l'ANSSI.

Cf. 2.1.4 pour la clause.

[8] https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/
[9] https://www.ssi.gouv.fr/guide/guide-des-bonnes-pratiques-de-linformatique/
[10] https://www.ssi.gouv.fr/guide/securiser-ladministration-des-systemes-dinformation/

2.1.4. Pièces contractuelles : clause type

Document : CCAP

ARTICLE X.X « Documents contractuels»

Le marché est constitué des documents contractuels suivants, par ordre de priorité :

- l'acte d'engagement et ses éventuelles annexes notamment financière;
- le CCAP (Cahier des Clauses Administratives Particulières) et ses éventuelles annexes ;
- le CCTP (Cahier des Clauses Techniques Particulières) et ses éventuelles annexes ;
- l'offre technique du titulaire et ses éventuelles annexes dont, le cas échéant, le plan d'assurance sécurité et/ou le plan de prévention des risques (PPR)].
- le cas échéant, les actes spéciaux de sous-traitance et leurs actes modificatifs, postérieurs à la notification du marché public ;
- le cas échéant, le formulaire d'engagement et de reconnaissance de responsabilité (document en annexe 2) ;
- le cas échant la PSSI [lister les éventuelles règlementations ; cf. point 2.1.3].
- [A COMPLETER]

2.2. Obligation de protection de l'information

Si les données ou informations échangées avec le titulaire sont concernées par l'instruction interministérielle n°901/SGDSN/ANSSI du 28 janvier 2015 ou par l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale, l'acheteur peut intégrer la clause de confidentialité ci-dessous, laquelle fait de toute information une information confidentielle contrairement au CCAG-TIC qui prévoit que ne sont confidentielles que les informations indiquées comme telles. Son choix dépend de la nature des données et du risque associé à leur divulgation / diffusion.

Document : CCAP

ARTICLE X.X « Obligations de confidentialité »

Confidentialité des informations :

Par dérogation à l'article 5.1.1 du CCAG-TIC, une information confidentielle désigne toute information de quelque nature (y inclus la méthodologie, la documentation, les informations ou le savoir-faire), sous quelque forme que ce soit (y inclus sous forme orale, écrite, magnétique ou électronique), sur tout support dont l'acheteur est propriétaire ou titulaire, et qui est communiquée au titulaire, ou obtenue de toute autre façon par ce dernier dans le cadre de ses relations avec l'acheteur. Le titulaire et son personnel, et le cas échéant ses sous-traitants, ne peut l'utiliser que pour l'accomplissement des prestations prévues au marché.

Toutefois, n'est pas considérée confidentielle toute information :

- qui était dans le domaine public au moment de sa divulgation ou que l'acheteur aurait lui-même rendue publique pendant l'exécution du marché ;
- signalée comme présentant un caractère non confidentiel et relative aux prestations du marché ;
- qui a été communiquée au titulaire du marché par un tiers ayant légalement le droit de diffuser cette information, comme le prouvent des documents existant antérieurement à sa divulgation par l'acheteur.

Les informations sensibles et celles de niveau Diffusion Restreinte (DR) doivent être protégées conformément à l'instruction interministérielle n° 901 relative à la protection des systèmes d'information sensibles[11].

□ En cas de manipulation d'informations classifiées de défense, le titulaire respecte l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense[12].

En cas de non-respect de l'obligation de confidentialité par le titulaire du marché, il faut prévoir des pénalités complémentaires à celles prévues à l'article 14 du CCAG-TIC voire à la résiliation du marché pour faute conformément à l'article 42 du CCAG-TIC (cf. le paragraphe 2.15 sur les pénalités).

[11] http://circulaires.legifrance.gouv.fr/pdf/2015/02/cir_39217.pdf

[12] Cette phrase n'est à insérer qu'en cas d'utilisation potentielle de données classifiées dans le cadre du marché public envisagé.

2.3. Maintien en condition de sécurité

Les politiques de sécurité convergent pour exiger les mises à jour des composants logiciels vers des versions supportées par l'éditeur ou la communauté Open Source qui les produisent.

Document : CCAP

ARTICLE X.X « Maintien en condition de sécurité »

En complément de l'article 31 du CCAG-TIC :

Traitement des obsolescences :

Le titulaire doit n'utiliser que des composants logiciels que l'éditeur s'engage à maintenir pendant la durée du marché. Si la durée du marché dépasse la durée pendant laquelle un éditeur s'engage à maintenir un composant logiciel, le titulaire maintient, livre et respecte une feuille de route de migration vers des systèmes maintenus.

Correctifs de sécurité :

Une vérification d'aptitude[13] ou une vérification de service régulier (VA et VSR) peut être refusée si des composants ne sont pas à jours des correctifs de failles de sécurité publiés depuis un délai supérieur à [**seuil à définir par l'acheteur**[14]]. L'acheteur définit les fréquences des livraisons en coordination avec les équipes d'exploitation, en fonction des différentes criticités des vulnérabilités concernées.
Le titulaire s'assure que l'application des correctifs de sécurité ne modifie pas les performances du système, en modifiant si besoin et à ses frais le système pour maintenir le niveau de performance malgré l'application du correctif

Le 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 réduire les risques, ou démontrer que les risques sont négligeables dans le contexte d'emploi.
Dans tous les cas le maintien en condition opérationnelle (MCO) et la tierce maintenance applicative (TMA) ou simplement l'hébergement incluent le maintien en condition de sécurité et donc la mise en œuvre des correctifs de failles de sécurité.

13 Ou vérification d'aptitude au bon fonctionnement (VABF).
14 Ce seuil contractuel doit être défini par une analyse de la valeur combinant l'enjeu opérationnel, le coût d'exploitation pour l'acheteur

2.4. Information sur les vulnérabilités et les incidents de sécurité touchant le SI du titulaire dans le cadre des prestations (développement, MCO, MCS, etc.)

Document : CCAP

ARTICLE X.X « Informations sur les vulnérabilités et les incidents de sécurité détectées sur le système d'information du titulaire »

Pour les prestations, produits et services fournis dans le cadre du marché, le titulaire met à disposition un dispositif d'information dédié à la sécurité informatique (notamment flux RSS/ATOM, liste de diffusion par courriel ou autre).

Ce dispositif vise à tenir l'acheteur informé des événements et changements impactant la sécurité, notamment liés à la connaissance d'une vulnérabilité impactant le système (annonce de correctif, attaque en cours, violation de données à caractère personnel si le traitement de données est sous-traité au titulaire), et des mesures correctives ou conservatoires à appliquer.

Afin de garder leur pouvoir d'alerte, ces canaux de diffusion ne sont pas mélangés avec des flux commerciaux et marketing. Ils peuvent être multiples dans le cas de fournitures en plusieurs composants mais sans laisser de vide d'information.
Réciproquement, les outils numériques mis à disposition permettent aux bénéficiaires et leurs experts SSI de signaler directement aux équipes appropriées du titulaire de possibles failles ou détournements de dispositifs de sécurité. Afin que ces signalements soient effectifs et efficaces, les conventions d'usage en cyber sécurité sont respectées (par exemple security.txt, abuse@).

2.5. Devoir de conseil

Document : CCAP

ARTICLE X.X « Devoir de conseil »

Le titulaire est tenu à une obligation permanente de conseil et de mise en garde, relative aux matériels, logiciels et prestations fournies à l'acheteur. Dans ce cadre, le titulaire notifie à l'acheteur toute information permettant d'améliorer le niveau de sécurité du système d'information et signaler les difficultés et risques que certains choix peuvent entraîner. Dans l'hypothèse où le titulaire ne respecte pas cette obligation, il ne peut se prévaloir d'une incohérence dans le marché pour s'exonérer de ses obligations contractuelles.

2.6. État de l'art

La sécurisation des systèmes informatiques dépend de l'évolution des technologies. Il appartient au titulaire de mettre en œuvre les pratiques de sécurité, d'employer les outils qui soient adaptés aux enjeux de sécurité de l'acheteur et proportionnés à la menace pouvant s'exercer sur les biens à protéger...

Document : CCAP

ARTICLE X.X « Etat de l'art»

Le titulaire garantit à l'acheteur qu'il est conforme à l'état de l'art pour les services et objets numériques fournis dans le cadre des prestations. A première demande, le titulaire fournit la preuve de cette conformité. Il précise alors les domaines concernés (interfaces web et courriels), les objets et bases d'information concernées (appareils connectés, sauvegardes de données, consoles d'administration). Le CCTP décrit les exigences que le titulaire doit respecter pour chaque service ou produit.

2.7. Cartographie des systèmes d'information

En fonction de l'objet du marché, des enjeux financiers, de la complexité, et de la sensibilité des données, il est recommandé que l'acheteur s'inspire des préconisations issues du guide « cartographie des systèmes d'information » de l'ANSSI[15] au sein du CCAP.

Document : CCAP

ARTICLE X.X « Cartographie des systèmes d'information»

Le titulaire dispose d'un inventaire et d'une cartographie des systèmes d'information dont il a la charge et doit les maintenir, selon les préconisations de l'ANSSI[16] issues du guide « cartographie des systèmes d'information », dans l'outil mis à sa disposition par l'acheteur. L'inventaire et la cartographie comprennent également la liste des « briques » matérielles et logicielles utilisées, ainsi que leurs versions exactes avec leur configuration. Ils comportent une base de données de configuration. La cartographie est livrée à la demande de l'acheteur et au minimum [fréquence à définir par l'acheteur[17]].

15 https://www.ssi.gouv.fr/guide/cartographie-du-systeme-dinformation/
24 https://www.ssi.gouv.fr/guide/cartographie-du-systeme-dinformation/
17 Une fréquence d'un an est raisonnable.

2.8. Mise à disposition des politiques et procédures de sécurité du titulaire

Document : CCAP

ARTICLE X.X « Mise à disposition des documents relatifs aux politiques et procédures de sécurité»

Le titulaire met à disposition de l'acheteur l'ensemble des documents relatifs aux politiques et procédures de sécurité à la demande de l'acheteur[18].

2.9. Gestion du personnel

Document : CCAP

ARTICLE X.X « Gestion du personnel »

En complément des articles 3.3 et 3.4 du CCAG-TIC, dès notification du marché et avant tout commencement d'exécution de celui-ci, le titulaire a obligation de transmettre à l'acheteur la liste des personnes contribuant à l'exécution de la prestation, ainsi que les engagements de reconnaissance de responsabilité signés (joint en annexe au CCAP).

En cas de sous-traitance, l'agrément du sous-traitant doit inclure l'engagement de reconnaissance de responsabilité signé par le sous-traitant en accompagnement de l'agrément du sous-traitant.

2.10. Sensibilisation du personnel

Document : CCAP

ARTICLE X.X « Sensibilisation du personnel du titulaire »

Le titulaire sensibilise son personnel, intervenant dans le cadre des prestations, à la sécurité de l'information, des systèmes d'information et aux règles de l'acheteur.

Le titulaire veille notamment à ce que son personnel intervenant dans le cadre de des prestations respecte les dispositions concernant la sécurité du présent marché.

[18] Permet des demandes répétées en cas de changement dans l'architecture du SI.

2.11. Remplacement du personnel

Document : CCAP

ARTCLE X.X « Remplacement du personnel »

En complément de l'article 3.4.2 du CCAG-TIC :

- En cas de départ définitif d'une personne nommément désignée, affectée par le titulaire à l'exécution des prestations du marché, le titulaire doit :
  - en aviser, sans délai, l'acheteur et prendre toutes dispositions nécessaires, afin d'assurer la poursuite de l'exécution des prestations ;
  - proposer à l'acheteur un remplaçant disposant de compétences au moins équivalentes et dont il lui communique le nom, les titres dans un délai d'un mois à compter de la date d'envoi de l'avis mentionné à l'alinéa précédent.
- Le remplaçant proposé par le titulaire est considéré comme accepté par l'acheteur, si celui-ci ne le récuse pas dans le délai d'un mois courant à compter de la réception de la communication mentionnée ci-dessus.
- Si l'acheteur récuse le remplaçant, le titulaire dispose d'un mois pour proposer un autre remplaçant.
- La décision de récusation prise par l'acheteur est motivée.

  A défaut de proposition de remplaçant par le titulaire ou en cas de récusation des remplaçants par l'acheteur et plus globalement en cas de non-respect de ses obligations contractuelles relatives au remplacement du personnel marché peut être résilié dans les conditions prévues à l'article 42.2 du CCAG-TIC[19].

  En aucun cas le remplacement du personnel ne peut justifier une augmentation des prix du marché.

  Pendant toute la durée d'exécution des prestations visées au présent marché, l'acheteur se réserve le droit de récuser les membres du personnel qui s'avéreraient inadaptés à l'exécution des prestations sur la base des résultats correspondant à une période d'essai d'un mois. Il motive sa décision après concertation avec le titulaire. Ce dernier procède au remplacement du personnel récusé dans les conditions précisées ci-dessus.

19 Si l'acheteur a fait référence au CCAG-PI, il faudra renvoyer à l'article 32.1 e) qui prévoit cette possibilité de résiliation pour faute.

2.12. Réversibilité et transférabilité

En fin de marché ou en cas de résiliation, le titulaire doit prémunir l'acheteur contre toute interruption ou baisse de la qualité des services avant la fin dudit marché. Dans le cas où un PAS est demandé, cette phase de transfert devra être décrite par le titulaire dans ce document. Sinon l'acheteur doit prévoir les modalités de transfert dans le CCTP. Le titulaire assure également l'ensemble des opérations pour que l'acheteur puisse reprendre les services dans de bonnes conditions (transfert de compétences, documentations, etc.).

Document : CCAP

ARTICLE X.X « Réversibilité et transférabilité »

Sécurité de la phase de transfert :

Le titulaire met en œuvre des mesures techniques et organisationnelles pour garantir la sécurité des données et des applications qui lui sont confiées, lors du transfert des prestations de la part du précédent titulaire en conformité avec les réglementations applicables.

- Durant la phase de transfert, l'assurance de la sécurité réside notamment dans :
  - La gestion des accès, habilitations ;
  - Le transfert de responsabilités ;
  - La fourniture d'informations nécessitant des mesures de protection adaptées ;
  - La gestion de la continuité de l'activité.

Commentaire : le précédent titulaire reste responsable de la sécurité jusqu'à la fin du transfert.

2.13. Propriété intellectuelle des résultats

Le CCAG-TIC propose deux options pour les clauses de propriété intellectuelle, qui peuvent être complétées en fonction des besoins :

- l'option A, applicable par défaut, qu'il est conseillé de compléter dans le CCAP,
- et l'option B, qui doit être obligatoirement complétée dans le CCAP.

Le choix de l'option nécessite d'identifier les résultats du marché susceptibles d'être protégés par des droits de propriété intellectuelle et de déterminer les besoins en termes d'utilisation de ces résultats.

Pour la rédaction des clauses de propriétés intellectuelles en lien avec les projets informatiques est traité dans le guide **«Achats informatiques et propriété intellectuelle »** élaboré de manière conjointe par l'APIE, la Direction interministérielle des systèmes d'information et de communication de l'État (DINSIC) et la Direction des achats de l'État (DAE)[20].

2.14. Pénalités

Document : CCAP

ARTICLE X.X « Pénalités »

Exemple :

En complément de l'article 14 du CCAG-TIC, en cas de violation des mesures de sécurité ou de l'obligation de confidentialité, le titulaire s'expose aux pénalités suivantes :

- en cas de non-respect des règles de sécurité et de protection des informations confidentielles n'impliquant pas des données à caractère personnel : application d'une sanction égale à 0,5 % du montant exécuté HT[21] du marché public à la date de constatation du fait générateur ;
- en cas de non-respect des règles de sécurité et de protection des informations confidentielles impliquant des données à caractère personnel : application d'une sanction égale à 2 % du montant exécuté HT[22] du marché public à la date de constatation du fait générateur.

En cas de constatation de plusieurs faits générateurs, les sanctions pécuniaires ainsi établies sont appliquées de façon cumulative.

Le montant des pénalités ainsi établies vient en déduction des paiements à effectuer au titre de toute facture afférente aux prestations exécutées à la date de survenance du fait générateur.

2.15. Résiliation

Document : CCAP

ARTICLE X.X « Résiliation »

Conséquences en cas de mise en cause du titulaire dans un incident de sécurité :

[20] https://www.economie.gouv.fr/files/files/directions_services/dae/doc/Guide_PII_web.pdf

21 Ce pourcentage pourra être défini par l'acheteur selon le montant du marché envisagé.

22 Ce pourcentage pourra être défini par l'acheteur selon le montant du marché envisagé.

En complément de l'article 42 du CCAG-TIC, en cas de non-respect des règles de sécurité, l'acheteur peut résilier pour faute le marché :

☐ avec mise demeure dans les conditions de l'article 42.2 du CCAG TIC

☐ sans mise en demeure

2.16. Destruction des données

En fonction de l'objet du marché et si l'acheteur a inclus l'IGI 1300 et / ou l'II 901 dans les pièces contractuelles, l'acheteur peut inclure ce type de clause sur la destruction des données :

Document : CCAP

ARTICLE X.X « Destruction des données »

Au terme du marché ou en cas de résiliation, le titulaire restitue sans délai à l'acheteur une copie de l'intégralité des données confiées par lui dans le cadre de la prestation. Une fois la restitution effectuée, le titulaire doit détruire, dans un délai de (**à compléter**), les éventuelles copies de données détenues dans son système d'information, y compris les données ayant fait l'objet de sauvegardes ou d'un archivage. La restitution et la destruction des données seront constatées par un procès-verbal daté et signé par le titulaire. Les procédés de destruction sont conformes aux réglementations en vigueur (instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale, instruction interministérielle N°901 relative aux mesures de protection des systèmes d'information traitant d'informations sensibles non-classifiées de défense de niveau Diffusion Restreinte (DR)

2.17. Audit de sécurité

Document : CCAP

ARTICLE X.X « audit de sécurité »

L'acheteur peut effectuer ou de faire effectuer un audit de sécurité auprès du titulaire ou le cas échéant de ses sous-traitants afin de s'assurer de la prise en compte effective du niveau de sécurité requis par l'acheteur.

Le titulaire est informé 15 jours à l'avance (date de l'audit, modalités financières pour l'acheteur et le titulaire, etc.).

L'acheteur, ou l'organisme mandaté à cette fin, peut, pendant une période de six mois à compter de la fin ou de la résiliation du marché, exercer un contrôle dans les locaux du

titulaire et, le cas échéant, dans ceux de ses sous-traitants afin de vérifier que les dispositions en matière de destruction des données ont été effectivement appliquées.

2.18. Décisions après vérifications

Document : CCAP

ARTICLE X.X « Décisions après vérifications »

En complément de l'article 26.1 du CCAG-TIC, les opérations de vérification qualitatives ont également pour objet de contrôler les conformités à la politique de sécurité.
L'acheteur apprécie l'enjeu du défaut eu égard à la sensibilité des données manipulées, leurs volumes, et les conséquences prévisibles si le défaut persiste.
En fonction de cette analyse, ces défauts peuvent avoir comme conséquence l'ajournement, le rejet ou la réception des prestations avec réfaction.

3. Clauses à intégrer dans le CCTP

Le CCTP est un document contractuel qui rassemble les clauses techniques d'un marché. L'objet de cette troisième partie est de fournir un ensemble de clauses aux acheteurs afin de l'aider à préciser les exigences de sécurité attendues par l'acheteur sur les différentes prestations.

Le tableau ci-dessous indique les types de clauses relevant du CCTP en fonction de l'objet du marché :

Objet du marché / Clauses du CCTP	Prestations intellectuelles (études, conseil, audit, etc.)	Hébergement externe	Achat de matériels et logiciels	Exploitation et supervision	Études et développement
Etat de l'art (§3.1)	☑	☑	☑	☑	☑
Obligations titulaires manipulant des informations de l'acheteur sur leur SI (§ 3.2)	☑	☑	☑	☑	☑
Obligations pour les titulaires intervenant au sein des locaux de l'acheteur (§ 3.3)	☑			☑	☑
Obligations pour les titulaires intervenant en situation d'astreinte (§ 3.4)		☑ (selon les besoins)		☑ (selon les besoins)	
Obligations en cas d'interconnexion entre les SI de l'acheteur et du titulaire (§ 3.5)		☑		☑	☑
Clauses d'études (§ 3.6.1)					☑
Clauses de développement (§ 3.6.2)					☑
Clauses d'hébergement (§ 3.6.3)		☑			
Clauses d'achat de matériels/logiciels (§ 3.6.4)			☑		

3.1. Etat de l'art

Document : CCTP

ARTICLE X.X « Etat de l'art »

Conformément à l'article XX du CCAP[23], le titulaire conçoit, met en œuvre et exploite les systèmes d'informations sous sa responsabilité conformément à l'état de l'art en matière de sécurité des systèmes d'information. Il doit se reporter systématiquement aux guides de recommandations de l'ANSSI pour être à jour de l'état de l'art en la matière. Toutefois, il doit respecter les exigences suivantes pour les services Web et de messagerie :

- Interfaces web
  - les développements ne doivent pas générer d'adhérence avec des modules spécifiques (Flash, Silverlight, JRE, etc.) ou une technologie en particulier ;
  - les mécanismes cryptographiques TLS (https) doivent être systématiquement activés pour identifier et authentifier la source et protéger les communications ; l'utilisation de la technologie HSTS est fortement recommandée ;
  - les mécanismes de protection des cookies de session (HttpOnly, Secure, SameSite) sont mis en œuvre pour se protéger des vols ou exploitation de sessions déjà ouvertes ;
  - une politique de sécurité des contenus (CSP, SRI) et des navigateurs (emploi d'entêtes de sécurité (X-Content-Type-Options, X-Frame-Options, X-XSS-Protection, Referrer-Policy) est élaborée pour se protéger contre les injections de contenus actifs malicieux ;
  - les obligations légales sont renseignées sur les sites Internet et un point de contact est publié via le fichier /.well-known/security.txt pour permettre des signalements directement auprès des points de contact identifiés.
- Services de courriels
  - les mécanismes de chiffrement TLS sont mis en œuvre pour l'authentification, la lecture et la distribution des messages (STARTTLS, SMTPS, IMAPS, etc.) ;
  - la mise en œuvre des mécanismes permettant de garantir l'authenticité des émetteurs est systématiquement envisagée (contrôle des noms de domaines associés aux serveurs (SPF),

[23] Cf. 2.5 du présent guide.

	signature numérique (DKIM), politique de sécurité liant le tout (DMARC)).

3.2. Obligations pour les titulaires manipulant des informations de l'acheteur sur leur SI

Lorsque le titulaire est amené à manipuler des informations de l'acheteur sur son propre système d'information, l'acheteur peut imposer des mesures complémentaires. Les clauses suivantes peuvent alors être intégrées au CCTP. Si un PAS est exigé, l'acheteur devra vérifier l'adéquation de la réponse du titulaire à l'exigence énoncée par l'acheteur dans le CCTP.

3.2.1. Spécifications techniques et utilisation de labels

L'acheteur définit ses besoins et les prestations à réaliser par référence à des spécifications techniques ou par l'utilisation de labels[24].

Ce sont en effet les articles R.2111-4 à R.2111-15 dudit code qui précisent ce point en indiquant que la formalisation du besoin est possible à travers :
- la formulation de spécifications techniques
- l'utilisation de labels

La notion de label et les conditions de recours sont précisées aux articles R.2111-12 à R.2111-15 : un label est tout document, certificat ou attestation qui prouve que les produits, les services, les procédés ou les procédures en rapport avec l'objet du marché remplissent certaines caractéristiques.

Il convient de noter que lorsqu'un acheteur exige un label particulier, celui-ci est tenu d'accepter les labels équivalents qui confirment que les caractéristiques exigées sont remplies voire tous autres moyens de preuve appropriés, lorsque le candidat n'a pas la possibilité d'obtenir le label spécifié par l'acheteur ou un label équivalent dans les délais fixés pour des raisons qui ne lui sont pas imputables[25].

Les visas de sécurité ANSSI : certification et qualification

Les visas de sécurité que délivre l'ANSSI permettent d'identifier le niveau de fiabilité des solutions de sécurité à l'issue d'une évaluation réalisée par des laboratoires agréés selon une méthodologie rigoureuse et éprouvée.
Ces visas se matérialisent, selon le contexte et le besoin, par une certification ou une qualification :

[24] Article L.21111-1 du code de la commande publique : «les travaux, fournitures ou services à réaliser dans le cadre du marché public sont définis par référence à des spécifications techniques.
[25] Cf. articles R.2111-16 et R.2111-17 du code de la commande publique.

- la certification : elle est l'attestation du niveau de robustesse d'un produit, basée sur une analyse de conformité et des tests de pénétration réalisés par un évaluateur tiers sous l'autorité de l'ANSSI, selon un schéma et un référentiel adaptés aux besoins de sécurité des utilisateurs et tenant compte des évolutions technologiques. L'ensemble du processus est géré au sein de l'ANSSI par le Centre de Certification National.

  Pour plus de précisions :

- https://www.ssi.gouv.fr/administration/produits-certifies/

- la qualification : elle est la recommandation par l'État français de produits ou services de cyber sécurité éprouvés et approuvés par l'ANSSI. Elle atteste de leur conformité aux exigences règlementaires, techniques et de sécurité promues par l'ANSSI en apportant une garantie de robustesse du produit et de compétence du prestataire de service, et d'engagement du fournisseur de solutions à respecter des critères de confiance.

  Pour plus de précisions :

- https://www.ssi.gouv.fr/administration/qualifications/

Dans certains cas, la réglementation impose de recourir à des produits ou prestataires de service qualifiés (RGS, LPM…). Dans les autres cas, les visas de sécurité ne peuvent qu'être conseillés.

Document : CCTP

ARTICLE X.X « Caractéristique(s) particulière(s) des prestations »

A COMPLETER, avec des spécifications techniques ou les labels exigés (normes, performances ou exigences fonctionnelles particulières ou label particulier (certificat, attestation, visas de sécurité de l'ANSSI dans le cadre de prestations relatives à des solutions de sécurité, etc.) afin d'attirer l'attention des candidats.
Ces informations doivent également être portées dans le CCTP.
Attention :

- *lorsqu'un acheteur exige un label particulier, celui-ci est tenu d'accepter les labels équivalents qui confirment que les caractéristiques exigées sont remplies voire tous autres moyens de preuve appropriés, lorsque le candidat n'a pas la possibilité d'obtenir le label spécifié par l'acheteur ou un label équivalent dans les délais fixés pour des raisons qui ne lui sont pas imputables*
- *si les spécifications techniques font référence à des normes, celles-ci doivent être accompagnées de la mention « ou équivalent »*

3.2.1. Politique, organisation, gouvernance

Les clauses suivantes doivent être intégrées dans le CCTP si le marché ne comporte pas de PAS. Dans le cas où un PAS est exigé, ces différents éléments font partie du plan-type et il n'est pas nécessaire d'intégrer les clauses de ce paragraphe.

Document : CCTP

ARTICLE X.X « Politique, organisation et gouvernance de la sécurité »

- Politique de sécurité du titulaire : le titulaire applique et fait appliquer à sous-traitants la politique de sécurité du présent marché. Cette politique de sécurité traite notamment des thèmes suivants :
  - Organisation de la Sécurité des SI ;
  - Application de la Politique de Sécurité des SI ;
  - Évaluation de la sensibilité et protection des documents ;
  - Gestion des ressources humaines ;
  - Sécurité physique des locaux et des salles informatiques ;
  - Architecture et exploitation des SI : réseaux, systèmes ;
  - Sécurité des postes de travail ;
  - Sécurité des supports numériques ;
  - Gestion des autorisations et contrôle d'accès logique aux ressources ;
  - Développement et maintenance des systèmes ;
  - Gestion des incidents et des alertes ;
  - Gestion de la continuité d'activité des SI ;
  - Conformité et démarche de contrôle interne ;
  - Localisation des données.
- Organisation de la sécurité adéquate : le titulaire définit une organisation de la sécurité afin de respecter l'ensemble des contraintes émises par l'acheteur.
- Existence d'un correspondant de sécurité : le titulaire désigne parmi son personnel un correspondant sécurité pour toute la durée de la prestation. Ce correspondant est notamment :
  - l'interlocuteur privilégié de l'acheteur pour toutes les questions relatives à la sécurité de la prestation, notamment dans le cadre d'investigations initiées par l'acheteur ou le titulaire suite à des incidents de sécurité opérationnels ;

(Chargé du maintien et de la mise en application du PAS.)

- ce correspondant est joignable aux horaires suivants **(A COMPLETER)**. Tout remplacement de ce correspondant doit être notifié à l'acheteur conformément à l'article XX du CCAP[26]. De plus, une suppléance de ce correspondant de sécurité doit être assurée pour pallier son indisponibilité.

- Mise en œuvre d'une gestion de risques et son suivi : le titulaire met en place une gestion des risques et assure un suivi permanent de son niveau de maîtrise de risques ainsi que du respect des politiques et règles de sécurité applicables sur le périmètre des prestations, y compris auprès de ses propres sous-traitants.

- Gestion de crise sécurité : sur son domaine de responsabilité SI, le titulaire applique le processus formalisé et opérationnel de gestion de crise, apte à assurer le traitement d'événements remettant en cause de façon inacceptable pour l'acheteur le respect des engagements de service et de sécurité SI contractualisés.

  Ce plan précise au minimum :

  - les principes d'escalade (critères de déclenchement, synoptique d'escalade) ;
  - la composition de la cellule de crise : fonctions et responsabilités des membres (acheteur et titulaire). La liste nominative des membres et de leurs suppléants est référencée dans un annuaire ;
  - les moyens dédiés à la gestion de crise (salle(s) de crise, procédures opérationnelles, moyens de communication).

3.2.2. Gestion des biens

Document : CCTP

ARTICLE X.X « Gestion des biens »

- Séparation des données de l'acheteur et des données d'autres clients : le titulaire conserve et traite les données de l'acheteur de manière séparée de ses propres données ou de données d'autres clients du titulaire. Le titulaire doit restreindre l'accès aux données de l'acheteur suivant le principe de restriction au besoin d'en connaître[27].

[26] Cf. paragraphe 2.12 du présent guide.
[27] L'acheteur doit donner ses performances dans le CCTP : droits d'accès, machines virtuelles séparées, disques séparés, machines physiques séparées…

- Protection de la documentation de l'acheteur sur support papier : le titulaire assure la protection de la documentation de l'acheteur sur support papier au sein des locaux, en la stockant dans des armoires ou des coffres fermés à clé/code par exemple, et sa destruction à la fin de la prestation.

- Modalités d'échanges d'informations : le titulaire garantit que les modalités de stockage et d'échanges d'informations par mail permettent d'en assurer la confidentialité et l'intégrité.

- Échange de supports : le titulaire garantit que les supports échangés ou à connecter sur un SI de l'acheteur n'intègrent aucun code malveillant et ont fait l'objet d'un test d'innocuité positif au moyen d'une attestation à fournir à l'acheteur.

- Transmission de fichiers sur un support physique : toute transmission de fichiers sur un support physique (DAT, CDROM, etc.), par courrier externe ou par porteur, donne lieu à un accusé de réception.

  Il doit respecter les règles de protection des informations et documents existant en vigueur au sein de l'acheteur.

  De plus, l'ensemble des opérations de transferts de disques durs, de supports d'archives ou de sauvegarde doit être inscrit dans un registre des opérations précisant :

  -l'émetteur et le destinataire ;

  - le détail des opérations de transferts et notamment le nombre, la date.

  Sur simple demande, ce registre est mis à la disposition de l'acheteur adjudicateur par le titulaire.

- Marquage des ressources techniques : le titulaire applique des règles de marquage sur les ressources techniques (matériels et logiciels informatiques, supports de stockage) et les supports papier pour faire savoir au personnel autorisé que ces éléments contiennent des informations sensibles ou classifiées.

- Supports de stockage hébergeant des données de l'acheteur : le titulaire conserve en lieu sûr les supports de stockage de données en fin de vie hébergeant des données de l'acheteur, en attendant de procéder à leur effacement ou à leur destruction avec des moyens adaptés visant à s'assurer qu'aucune donnée ne puisse être récupérée.

  Le cas échéant, le titulaire ne met pas au rebut ou ne fait pas emporter par une société de maintenance, ou encore réutilise ces supports de sauvegarde à d'autres fins que celles prévues initialement sans l'autorisation expresse de l'acheteur.

- Maintien à jour et mise à disposition des données relatives à la prestation : le titulaire maintient à jour et est en mesure de mettre à disposition de l'acheteur toutes les données relatives à la prestation.

Le titulaire fournit systématiquement toute la documentation générée dans le cadre de la prestation à l'acheteur pour archive.

NB : le titulaire peut tenir un référentiel de toutes les données liées à la Prestation.

3.2.3. Sécurité physique

Document : CCTP

ARTICLE X.X « Sécurité physique »

- Changement de localisation géographique des services et des données : en cas de changement de localisation des données ou services, le titulaire en informe préalablement l'acheteur.
- Hébergement de données : à première demande de l'acheteur, le titulaire identifie tous les titulaires techniques hébergeant ou stockant les données et leurs copies, utilisées ou échangées en cours de marché ainsi que leur localisation.
- Contrôle d'accès physique aux bâtiments du titulaire : les bâtiments du titulaire hébergeant son personnel dans le cadre de la prestation doivent être équipés d'un dispositif de contrôle d'accès individuel. Les accès physiques aux bâtiments en question doivent être restreints aux stricts besoins opérationnels des différentes populations présentes dans les locaux du titulaire.

  Le titulaire dispose d'une procédure de gestion des accès physiques aux bâtiments du titulaire. Celle-ci précise au minimum les modalités de gestion des demandes et de suppressions d'accès.

  Le titulaire dispose d'une organisation relative à la gestion et au suivi des autorisations d'accès pour les bâtiments du titulaire.
- Contrôle des accès aux ressources techniques du titulaire : le titulaire garantit que les accès physiques aux salles informatiques sont strictement restreints aux besoins opérationnels des différentes populations présentes sur les sites utilisés dans le cadre de la prestation. Les accès sont équipés d'un dispositif de contrôle d'accès individuel.

  Le titulaire dispose d'une procédure de gestion des accès physiques aux locaux techniques du titulaire. Celle-ci précise au minimum les modalités de gestion des demandes et suppressions d'accès.

  Le titulaire dispose d'une organisation relative à la gestion et au suivi des autorisations d'accès pour les locaux hébergeant des ressources de l'acheteur et

les équipements de sûreté.

- Protection intrusion physique des locaux techniques du titulaire : les locaux du titulaire qui hébergent ses ressources techniques (serveurs, équipements informatiques, équipements réseaux / télécoms, etc.) sont équipés de moyens de :
- Protection contre l'intrusion et les effractions ;
- Détection d'intrusion et d'effraction reliés à un système de surveillance centralisé ;
- Réaction en cas d'intrusion ou d'effraction.

Ces équipements sont opérationnels 24h/24h et 7j/7j.

Les moyens de protection sont adaptés aux moyens de détection et de réaction.

En particulier, toutes les portes donnant sur l'extérieur du bâtiment ont une méthode automatique de détection d'ouverture. De plus, toute fenêtre raisonnablement accessible est protégée contre les intrusions.

- Accompagnement des visiteurs : le titulaire dispose d'une procédure spécifique à l'accueil des personnes étrangères à l'organisme. Il dispose également d'une procédure pour l'accès des véhicules au site.

  En particulier, les personnes extérieures nécessitant un accès aux salles hébergeant des ressources informatiques (techniciens, visiteurs, maintenance, etc.) sont accompagnées par une personne habilitée.
- Protection des plateaux mutualisés : en cas de mutualisation de ses plateaux, le titulaire met en place les mesures pour protéger les espaces attribués pour la prestation effectuée pour l'acheteur (accès au poste par badge, blocage session automatique après un certain temps d'inutilisation, câble de sécurité pour le matériel fourni par l'acheteur, etc.).
- Étanchéité physique des ressources informatiques : les salles hébergeant les ressources informatiques utilisées dans le cadre de la prestation ne partagent pas le même bâtiment avec d'autres fonctions, particulièrement des bureaux n'appartenant pas à l'organisation. Si l'espace doit être mutualisé pour des raisons économiques, alors la salle hébergeant des ressources informatiques utilisées dans le cadre de la Prestation de l'acheteur n'a pas de murs adjacents à d'autres bureaux.

  Le titulaire met en place des moyens garantissant une étanchéité physique entre les infrastructures physiques dédiées à l'acheteur de celles des autres clients au sein des salles informatiques :
- La salle hébergeant des matériels de l'acheteur doit si possible lui être dédiée ;
- Dans le cas où la séparation physique des salles n'est pas possible, le titulaire fournit à l'acheteur une solution de « suite privative » au sein de la salle multi-clients, isolée physiquement du reste de la salle par un grillage descendant plus bas que le faux plancher et montant plus haut que le faux plafond.

3.2.4. Sécurité des réseaux et de l'exploitation

Document : CCTP

ARTICLE X.X « Sécurité des réseaux et de l'exploitation »

- Cloisonnement des environnements informatiques[28] : le titulaire est garant du bon cloisonnement (physique ou logique) des environnements utilisés dans le cadre de la prestation.
- Sécurisation des flux d'administration[29] : le titulaire chiffre tous les flux d'administration (système et fonctionnelle) par des procédés fiables garantissant la confidentialité et l'intégrité des données. Par ailleurs, les postes d'administration utilisés pour la prestation doivent être dédiés et n'avoir accès ni à Internet, ni à aux infrastructures bureautique du titulaire.
- Règles de sécurité et d'exploitation : l'installation, l'exploitation et l'administration des moyens mis en œuvre dans le cadre des prestations sont conformes aux bonnes pratiques et aux règles de sécurité et d'exploitation établies par l'acheteur. Toute exception fera l'objet d'un accord préalable écrit des équipes de l'acheteur.
- Anti-virus opérationnel et à jour : le titulaire s'assure de la bonne installation et mise à jour d'un logiciel anti-virus sur tous les postes de travail et serveurs dont il est responsable dans le cadre de la prestation.

  La désactivation, même temporaire, d'un antivirus sur un serveur utilisé dans le cadre de la prestation devra avoir été préalablement notifiée à l'acheteur.
- Gestion des mises à jour : le titulaire gère les mises à jour et l'application des correctifs de sécurité et des mises à jour antivirales, pour assurer le maintien en condition opérationnelle de l'ensemble de ses équipements pour les services fournis à l'acheteur.
- Sauvegarde des données : le titulaire met en place un système de sauvegarde permettant la sauvegarde des données de la prestation hébergées sur les serveurs du titulaire conformément aux besoins de sauvegarde exprimés par le chef de projet de l'acheteur dans le cadre de la Prestation.

  Des tests périodiques (a minima semestriels) de restauration des sauvegardes effectuées sur les données contenues dans les serveurs du titulaire sont formalisés et effectués.

[28] https://www.ssi.gouv.fr/guide/securiser-ladministration-des-systemes-dinformation/
[29] https://www.ssi.gouv.fr/administration/guide/recommandations-de-securite-relatives-a-la-tele-assistance/

- Stockage des sauvegardes informatiques : le titulaire protège les sauvegardes informatiques en les stockant dans un coffre étanche et ignifuge pour les supports magnétiques, ou sur un site de back up sécurisé.

- Comptes individuels[30] : le titulaire s'assure que son personnel devant accéder à des ressources informatiques ou réseau dans le cadre de la prestation (qu'elles soient hébergées chez le titulaire ou chez l'acheteur) dispose d'un compte individuel qui peut être :

  - soit un compte nominatif qui lui est personnel et qui ne sera utilisé uniquement par cette personne tout au cours de la vie du compte ;
  - soit un compte individualisé qui pourra être attribué à des personnes différentes au cours de la vie du compte tout en n'étant toujours attribué qu'à une seule personne à la fois.

- Comptes obsolètes ou par défaut ; le titulaire s'assure de la suppression de tous les comptes inutiles ou obsolètes. De même, les mots de passe par défaut d'usine devront être systématiquement modifiés.

- Comptes techniques : dans le cadre de la cartographie du système d'information prévue à l'article XX du CCAP31, le titulaire doit fournir un inventaire justifié des comptes techniques (le compte propriétaire du fichier de la base de données, des données du serveur WEB, ...) nécessaires au fonctionnement du système.

- Recensement des comptes d'accès : le titulaire tient à jour la liste exhaustive des comptes d'accès au SI de l'acheteur existants ainsi que des rôles et privilèges qui y sont associés.

  Il fournit cette liste à l'acheteur sur demande.

  Le titulaire effectue et formalise une revue périodique* des comptes d'accès aux serveurs et autres ressources du titulaire utilisées dans le cadre de la prestation.

  *une revue « d'emploi » (a minima trimestrielle), une revue de « besoin » (a minima annuelle).

- Politique du moindre privilège[32] : le titulaire s'assure que tous les comptes (accès Windows et autres…) des intervenants dans le cadre de la prestation sont habilités selon le principe du moindre privilège.

- Attaques en essai et erreurs sur secrets d'authentification : les moyens d'authentification mis en place par le titulaire (sur ses serveurs,

[30] Les comptes concernés par cette exigence sont bien ceux gérés par le titulaire.
[31] Cf. le paragraphe 2.6 du présent guide.
[32] Le principe du moindre privilège est le principe selon lequel chaque intervenant doit disposer d'un compte ayant exactement les droits nécessaires à l'accomplissement de ses tâches.

applications et postes de travail) incluent une protection contre les attaques en essai et erreur sur les secrets d'authentification[33].

- Journalisation des actions : le titulaire conserve de manière exploitable, sur une durée d'un an après la fin de la prestation, la trace des actions réalisées dans son système à des fins de contrôle (audit) et de preuves.

  Le titulaire collecte et stocke à minima les informations suivantes :

  - connexion et déconnexion aux équipements et applications ;
  - consultations d'informations relatives à la vie privée ;
  - informations d'usage de l'Internet (accès aux sites Web) ;
  - accès en lecture et/ou en écriture à des fichiers et dossiers marqués « CONFIDENTIEL » ;
  - informations concernant les accès fructueux et infructueux (identifiant de l'utilisateur, date, heure) aux serveurs du titulaire.

  Les traces enregistrées par le titulaire doivent être imputables à un individu, elles sont par ailleurs horodatées selon une référence horaire commune à l'ensemble des équipements d'un même réseau.

- Gestion des traces : le titulaire prévoit dans sa procédure de traitement d'incident un chapitre sur la préservation des traces éphémères (volatiles) en cas de suspicion d'attaque. Une trace volatile est une trace potentiellement utile pour l'analyse forensique d'une attaque informatique mais qui ne peut pas, par nature, être journalisée (contenu de la RAM, du swap, journal des transactions d'un système de fichier, divers dates liées aux fichiers, clés de registres…). La procédure établit comment limiter l'activité susceptible de détruire ces traces éphémères.

- Politique de mot de passe : le titulaire respecte la politique de définition des mots de passe de l'acheteur[34] sur l'ensemble des comptes d'accès utilisateurs aux postes de travail et applications sous la responsabilité du titulaire.

- Sources d'installation des logiciels : le titulaire dispose des sources d'installation des logiciels utilisés dans le cadre de la prestation, lorsque ces logiciels ne sont pas mis à disposition par l'acheteur.

- Validité des licences : le titulaire s'assure de la bonne validité des licences des logiciels qu'il met à disposition de son personnel ou de l'acheteur dans le cadre de la prestation.

[33] Exemple de mesure de protection : blocage pendant 30 minutes de la session d'un poste de travail après 3 tentatives de connexion échouées.

[34] Cf le guide correspondant : https://www.ssi.gouv.fr/guide/mot-de-passe/

3.2.5. Sécurité du poste de travail

Document : CCTP

ARTICLE X.X « Sécurité du poste de travail »

- Protection contre le vol des postes de travail : le titulaire met en place des mécanismes de protection pour prévenir le vol des postes de travail. Le titulaire met notamment en place des câbles antivol de façon systématique.
- Chiffrement du poste de travail : une solution de chiffrement, si possible qualifiée, est mise à disposition par le titulaire à ses intervenants afin de chiffrer les données sensibles stockées sur les postes de travail, les serveurs, les espaces de travail, ou les supports amovibles.

3.2.6. Traitement des incidents

Document : CCTP

ARTICLE X.X « Traitement des incidents »

- Remontée d'alerte : le service de supervision du titulaire met en place un système de remontée d'alerte à l'acheteur, afin de détecter tout comportement anormal sur un périmètre SI lié à la prestation (ex : montée en charge du réseau), vol ou perte d'informations sensibles appartenant à l'acheteur (documentations technique en particulier).
- Enregistrement et traçabilité et gestion des incidents de sécurité : le titulaire assure l'enregistrement et la traçabilité des incidents de sécurité et dispose d'un processus formalisé et opérationnel de gestion des incidents de sécurité sur son domaine SI.
- Traitement des incidents de sécurité : le titulaire contacte les interlocuteurs sécurité de l'acheteur désignés pour signaler tout incident de sécurité SI susceptible d'affecter les données ou le SI de l'acheteur. De plus :
  - si cet incident a lieu sur le SI de l'acheteur, le titulaire participera à la demande de l'acheteur au traitement de l'incident ;
  - si cet incident a lieu sur le SI du titulaire, le titulaire autorisera l'acheteur ou un tiers désigné à participer au traitement de l'incident (si l'acheteur le souhaite).

En outre, des réunions périodiques d'analyse post-incident devront être planifiées avec l'acheteur (traitement des causes profondes).

- Base de connaissance : le titulaire capitalise les procédures de résolution des problèmes techniques récurrents dans une base de connaissance dédiée qu'il fournit à l'acheteur sur demande.

3.2.7. Disponibilité des données et des systèmes d'information

Document : CCTP

ARTICLE X.X « Disponibilité des données et des systèmes d'information »

Durant le marché, le titulaire maintient la disponibilité des données (quel que soit leur support), leur conservation et la disponibilité des systèmes d'information dans un délai maximum de (**à compléter**)[35].

En cas de non-respect de ces délais, l'acheteur applique les pénalités visées à l'article XX du ***(à choisir : CCAP[36]/CCAG-TIC)***.

L'acheteur doit préciser les performances de disponibilité attendues dans le CCTP et mettre en cohérence, si besoin, l'article 14.2 du CCAG-TIC relatif aux pénalités pour indisponibilités, s'il a fait référence à ce CCAG.

3.2.8. Continuité des services

En fonction de l'objet du marché, des enjeux financiers, de la complexité, et de la sensibilité des données, l'acheteur peut exiger que le soumissionnaire fournisse un plan de continuité d'activité (PCA) et décrit dans le CCTP les éléments précis devant figurer a minima dans le PCA.
L'acheteur doit détailler dans le CCTP la procédure d'alerte à respecter par le titulaire en cas d'incident affectant la continuité des services.

Document : CCTP

ARTICLE X.X « Continuité des services »

- Plan de continuité d'activité : le titulaire assure la disponibilité de l'ensemble des services liés à la prestation tout au long du contrat dans les délais maximum suivants : (**A COMPLETER**)[37]. Il fournit, à la demande de l'acheteur, la preuve de l'existence d'un plan de continuité d'activité

[35] L'acheteur doit définir ces délais dans le CCAP pour que cette clause puisse s'appliquer.
[36] Cf. le paragraphe 2.14 du présent guide.
[37] L'acheteur doit définir ces délais dans le CCAP pour que cette clause puisse s'appliquer.

régulièrement testé pour l'ensemble des services fournis à l'acheteur. L'acheteur se réserve le droit de demander les résultats des exercices de continuité d'activité réalisés régulièrement par le titulaire.

- Remplacement du matériel endommagé ou perdu : le titulaire prend toutes les dispositions nécessaires (matériel en spare, contrats de service), en relation avec l'acheteur, pour remplacer rapidement et sur les différents sites de l'acheteur tout matériel sous sa responsabilité endommagé ou perdu (poste de travail, serveur, équipement réseau).

  Incident affectant la continuité des services : En cas d'incident affectant la continuité des services, le titulaire signale l'événement à l'acheteur selon la procédure d'alerte qu'il a définie à l'article XX du CCTP (directive de gestion des alertes, incidents et situations de crise).

3.2.9. Conformité, audit, inspection, contrôle

Document : CCTP

ARTICLE X.X « Conformité, audit, inspection, contrôle »

- Autocontrôles de sécurité : le titulaire effectue des autocontrôles de conformité aux exigences du **(à choisir CCTP/PAS)** pour garantir le niveau de sécurité au démarrage de la prestation ainsi que son maintien tout au long de la prestation.

- Régularisation des écarts ou des non-conformités au niveau d'exigence de sécurité de l'acheteur : **(en cas de constatation d'écarts avec le PAS et, plus généralement,)**[38] en cas de non-conformité au niveau d'exigence de sécurité requis par l'acheteur, un plan de remédiation devra être formalisé par le titulaire 15 jours après la constatation des écarts. Le titulaire doit ensuite régulariser ces écarts par l'application du plan de remédiation dans un délai convenu en commun accord entre les deux parties.

La fréquence minimale est définie dans le contrat. Sur la base de ces contrôles effectués, le titulaire doit rendre compte des résultats à l'acheteur à l'occasion de comités de sécurité.

NB : les retards peuvent donner lieu à des pénalités financières. Par ailleurs, des écarts trop importants peuvent être une cause de rupture de contrat.

[38] A ne mettre que si l'acheteur a demandé un PAS.

3.3. Obligations pour les titulaires intervenant au sein des locaux de l'acheteur

Lorsque le titulaire est amené à intervenir au sein des locaux de l'acheteur, il doit, au même titre que les agents, respecter un ensemble de règles. Les clauses suivantes peuvent alors être intégrées au contrat.

Document : CCTP

ARTICLE X.X « Obligations relatives à l'intervention du titulaire dans les locaux de l'acheteur »

- Respect des exigences de sécurité de l'acheteur : au même titre que les agents de l'acheteur, le titulaire doit prendre connaissance et appliquer les règlements internes de l'acheteur (PSSI, directive d'utilisation des systèmes d'information, directive d'utilisation de la messagerie, etc.).
- Respect des standards et méthodologies de l'acheteur : le titulaire doit respecter les standards et les méthodologies préconisés au sein de l'acheteur.
- Respect du périmètre de la prestation : le titulaire ne tente pas d'accéder à des informations ou des ressources informatiques ne faisant pas partie du périmètre de la prestation.
- Connexion d'équipements au réseau de l'acheteur : le titulaire doit connecter sur le réseau interne de l'acheteur uniquement des équipements fournis par l'acheteur. Cela comprend tout type de matériel y compris les supports de stockage amovibles (clés ou disques dur USB, etc.)
- Inventaire des composants mis à disposition par l'acheteur : le titulaire met en place une solution pour élaborer et maintenir un inventaire complet et à jour des composants mis à disposition par l'acheteur. Cette liste devra être transmise régulièrement à l'acheteur
- Recensement des comptes d'accès : le titulaire tient à jour la liste exhaustive des comptes d'accès au SI de l'acheteur existants ainsi que des rôles et privilèges qui y sont associés.

  Il doit être en mesure de fournir cette liste à l'acheteur sur demande.

  Le titulaire doit également effectuer et formaliser une revue périodique* des comptes d'accès aux serveurs et autres ressources du titulaire utilisées dans le cadre de la Prestation.

  *une revue « d'emploi » (a minima trimestrielle), une revue de « besoin » (a minima annuelle).
- Restitution des équipements fournis par l'acheteur : à la fin de la prestation, le titulaire doit restituer l'ensemble du matériel fourni par l'acheteur.

- Restitution des informations collectées par le titulaire : à la fin de la prestation, le titulaire doit restituer ou détruire les informations de l'acheteur en sa possession. Un procès-verbal de destruction des données doit être signé par le titulaire.
- Transfert de connaissances : le titulaire doit préciser la date exacte de départ des intervenants de la prestation et organiser le transfert de connaissances auprès des équipes de l'acheteur.

3.4. Obligations pour les titulaires intervenant en situation d'astreinte

Dans le cadre de certaines prestations, il peut être demandé aux titulaires d'assurer des astreintes, pendant lesquelles ils peuvent être amenés à se connecter à leur SI voire au SI de l'acheteur à distance et en horaires non ouvrés. Les clauses suivantes peuvent alors être intégrées au contrat.

Document : CCTP

ARTICLE X.X « Obligations relatives aux astreintes »

- Astreinte : le titulaire prévoit un dispositif garantissant les services d'astreinte nécessaires à la continuité de service et à la tenue des engagements. Les cas de force majeure doivent également être couverts.
- Sécurisation des flux d'astreinte : le titulaire met en œuvre un tunnel sécurisé avec chiffrement des communications (ex. VPN, IPSec) pour la connexion à distance en astreinte aux réseaux utilisés dans le cadre de la Prestation (que ce soient ceux du titulaire, ceux de l'acheteur ou les deux éventuellement). Le personnel du titulaire devra explicitement lancer la connexion et s'authentifier pour obtenir l'accès aux SI à distance (connexion authentifiée non permanente) ou utiliser les services d'accès distants mis à disposition par l'acheteur.
- Chiffrement des postes d'astreinte : le titulaire met en œuvre le chiffrement intégral du poste de travail utilisé en astreinte.
- Authentification forte : le titulaire rend obligatoire l'utilisation de l'authentification forte (ex. badge, token) au poste de travail utilisé en astreinte.

  Connexion distante : le titulaire restreint la connexion distante aux personnels d'astreinte, aux horaires d'astreintes définis (ex. connexion non autorisée en horaires ouvrés), et aux ressources nécessaires en astreinte uniquement.

- Enregistrement des accès : Dans le cas où l'acheteur autorise la Prise en Main À Distance (PMAD) de ses infrastructures, le titulaire enregistre et sécurise les accès distants au SI de l'acheteur.
- Suivi des interventions : le titulaire est capable de fournir à l'acheteur, sur demande, la liste de son personnel avec son nom, prénom et adresse mail, qui est intervenu à un instant donné sur le SI de l'acheteur en astreinte.

N.B : pour l'ensemble des interventions réalisées généralement hors heures ouvrées, l'acheteur assurera une tolérance d'accessibilité au SI de production à partir d'un site externe au lieu normal d'exécution de la mission. Toutefois, les agissants devront être spécialement identifiés et disposer d'une formation/sensibilisation conforme aux attentes de sécurité.

3.5. Obligations en cas d'interconnexion entre les SI de l'acheteur et du titulaire

Dans le cadre de certaines prestations, une interconnexion est réalisée entre les SI de l'acheteur et du titulaire. Cette interconnexion doit être cadrée avec vigilance. Ce paragraphe liste un ensemble de points de vigilance à considérer dans la rédaction de ce type de contrat.

Document : CCTP

ARTICLE X.X « Obligations relatives à l'interconnexion entre les SI de l'acheteur et du titulaire »

- Respect des exigences de sécurité de l'acheteur : au même titre que les agents de l'acheteur, le titulaire prend connaissance et applique les règlements internes de l'acheteur (PSSI, directive d'utilisation des systèmes d'information, directive d'utilisation de la messagerie, etc.).
- Respect des standards et méthodologies de l'acheteur : le titulaire respecte les standards et les méthodologies préconisés au sein de l'acheteur et figurant en annexe du présent CCTP.
- Respect du périmètre de la prestation : le titulaire ne doit pas tenter d'accéder à des informations ou des ressources informatiques ne faisant pas partie du périmètre de la prestation.
- Interconnexion des SI de l'acheteur et du titulaire : en cas d'interconnexion des SI de l'acheteur et du titulaire, le titulaire doit prendre les mesures de sécurité nécessaires afin de maintenir le niveau de sécurité global des SI. L'interconnexion devra être réalisée via des infrastructures d'accès validées par l'acheteur au travers d'une étude ciblée, dans le respect du cadre technique et des règles de sécurité de l'acheteur.

Pour chaque interconnexion, les éléments suivants doivent être définis :

- les flux et protocoles autorisés, ainsi que les ressources auxquelles le titulaire est autorisé à accéder au travers de la zone « partenaires ». Ces éléments doivent être restreints au strict nécessaire ;
- les modalités d'authentification requises : authentification par mot de passe, authentification forte par mot de passe unique ou par certificat ;
- les modalités de chiffrement des échanges : le chiffrement des flux transitant sur Internet est requis ;
- les exigences spécifiques de traçabilité des accès ;
- les moyens de sécurité supplémentaires à mettre en œuvre : contrôle de conformité, outils de détection ou de prévention d'intrusion, contrôle de contenu, filtrage applicatif…

3.6. Clauses spécifiques aux typologies de prestation

3.6.1. Prestations d'études

Les prestations d'études nécessitent l'intégration de certaines clauses spécifiques. Ce paragraphe liste un ensemble de points de vigilance à considérer dans la rédaction de ce type de contrat.

Les prestations d'études représentent ici toutes les prestations faisant intervenir des titulaires en phase projet (des phases d'étude des besoins aux phases de test en passant par les phases de conception), sans action de développement.

Document : CCTP

ARTICLE X.X « Obligations spécifiques liées aux prestations d'étude »

- Respect des standards et méthodologies de l'acheteur : le titulaire doit respecter les standards et les méthodologies préconisés au sein de l'acheteur. En particulier, le titulaire doit appliquer les méthodes d'évaluation de la sensibilité et d'analyse de risques des systèmes d'information lorsqu'il intervient dans les phases amont des projets.
- Ségrégation des environnements : le titulaire doit utiliser différents environnements cloisonnés pour les activités de développement, de recette et de pré-production.
- Conduite des tests : lors de la conduite de tests de validation ou du déploiement, le titulaire doit :
  - utiliser des données de tests anonymisées (sauf accord explicite de l'acheteur) ;
  - ne pas provoquer de perturbations du système d'information de

l'acheteur lors des séances de test ;

- remettre en l'état initial les systèmes testés et réinitialiser le matériel sensible.

3.6.2. Prestations de développement

Les prestations de développement nécessitent l'intégration de certaines clauses spécifiques. Ce paragraphe liste un ensemble de points de vigilance à considérer dans la rédaction de ce type de contrat.

Document : CCTP

ARTICLE X.X « Obligations spécifiques liées aux prestations de développement »

- Utilisation du cadre standard de développement : le titulaire doit utiliser le cadre commun de développement (méthodes, démarches, etc.) de l'acheteur comprenant notamment :
  - l'organisation des équipes de développement et de la prestation ;
  - les configurations matérielles préconisées pour le développement ;
  - les outils de développement préconisés par l'acheteur (logiciels, versions, etc.) ;
  - une structure de développement (framework) intégrant les fonctions de sécurité.
- Propriété du code : l'acheteur est propriétaire du code et des droits de propriété intellectuelle des éléments développés dans le cadre de la prestation.
- Ségrégation des environnements : le titulaire doit utiliser différents environnements cloisonnés pour les activités de développement, de recette et de pré-production.
- Protection des codes sources : le titulaire doit mettre en œuvre les mesures de sécurité nécessaires et adéquates à la protection des codes sources.
- Documentation du code : le titulaire doit commenter et documenter le code développé dans le cadre de la prestation. La documentation doit être mise à jour régulièrement.
- Traçabilité des actions de développement : toute activité de développement doit être tracée et conservée dans un format facilitant son exploitation ultérieure.

- Sauvegarde des codes sources : le titulaire doit sauvegarder et conserver chaque version du code source recettée dans le cadre de la prestation. Les accès à ces sauvegardes devront être tracés.
- Dépôt des codes source : le titulaire doit déposer les codes sources dans ses différentes versions et mises à jour selon les recommandations de l'acheteur.
- Conduite des tests : lors de la conduite de tests de validation ou du déploiement, le titulaire doit :
  - utiliser des données de tests anonymisées ;
  - ne pas provoquer de perturbations du système d'information de l'acheteur lors des séances de test ;
  - remettre en l'état initial les systèmes testés et réinitialiser le matériel sensible
  - ne pas introduire de régression vis-à-vis d'un état de sécurité atteint dans une version précédente
- Contrôle de la qualité et de la sécurité du développement : l'acheteur se réserve le droit de contrôler la qualité et la sécurité du développement fourni par le titulaire, via des audits et/ou des tests d'intrusion par exemple (audit de code sur les parties les plus sensibles, etc.).

3.6.3. Prestations d'hébergement

Les prestations d'hébergement nécessitent l'intégration de certaines clauses spécifiques qui peuvent être basée sur les exigences de la directive de sécurité de l'hébergement informatique de l'acheteur.

Document : CCTP

ARTICLE X.X « Obligations spécifiques liées aux prestations d'hébergement »

- Respect de la directive de sécurité de l'hébergement informatique de l'acheteur : le titulaire doit respecter les exigences de la directive de sécurité de l'hébergement informatique de l'acheteur.

3.6.4. Prestations d'achat de matériels/logiciels

Les contrats d'achat de matériels et logiciels nécessitent l'intégration de certaines clauses spécifiques. Ce paragraphe liste un ensemble de points de vigilance à considérer dans la rédaction de ce type de contrat.

- Absence de failles à la mise en production : le titulaire s'engage à ce que les produits du contrat soient, au jour de leur mise en production pour l'acheteur, dépourvus de toute faille, faiblesse ou défaut de conception portant atteinte à la sécurité des informations.

- Détection d'une vulnérabilité : en cas de mise en évidence d'une vulnérabilité affectant un produit du contrat, le titulaire doit mettre à disposition de l'acheteur dans les meilleurs délais une solution de contournement ou une solution palliative (mise à disposition de correctifs) n'affectant ni les performances ni les fonctionnalités du produit concerné. Le titulaire collabore également avec l'acheteur pour déterminer l'origine de la vulnérabilité et les actions à engager pour l'éradiquer.

- Exigences liées à la maintenance : dans le cadre d'une opération de maintenance, le titulaire s'engage à chiffrer ou effacer de manière sécurisée toutes les données avant l'envoi en maintenance externe de toute ressource informatique de l'acheteur.

  Si les données ne sont pas sensibles, et si elles ne peuvent être chiffrées ou effacées en totalité (par exemple : disque dur défectueux sous garantie), l'envoi en maintenance externe ne peut se faire que sous couvert d'un engagement de confidentialité de la part du mainteneur, ou bien dans le cadre d'une réparation sur site en présence d'un membre de l'équipe locale chargée des systèmes d'information.

  Si les données sont sensibles et si elles ne peuvent être chiffrées ou effacées en totalité, l'envoi en maintenance externe est interdit.

- Exigences liées à la télémaintenance[39] : dans le cadre d'un accès de télémaintenance à une ressource informatique (matériel, logiciel) de l'acheteur, le titulaire doit présenter des mesures de sécurité renforcées validées par l'acheteur.

Exigences liées à la qualification

En cas d'achat de produits de sécurité qualifiés, il est nécessaire de se référer au guide d'achat des produits qualifiés de l'ANSSI. Si le produit vise une qualification après la notification du marché, il est fortement recommandé que le jalon J0 du processus de qualification soit franchi préalablement.

Exemples de mesures de sécurité renforcées :

- Sécurisation de l'infrastructure de raccordement réseau (cf. Obligations en cas d'interconnexion entre les SI de l'acheteur et du titulaire) ;
- Mise en place de mots de passe spécifiques pour l'accès en télémaintenance, respectant des règles de robustesse et de renouvellement ;
- Activation sur demande des accès entrant en télémaintenance. Par défaut, les accès entrants doivent être inactifs ;
- Journalisation des accès en télémaintenance ;

39 https://www.ssi.gouv.fr/administration/guide/recommandations-de-securite-relatives-a-la-tele-assistance/

- Interdiction des possibilités de rebond depuis l'accès en télémaintenance vers le reste du réseau local de l'acheteur et plus largement vers les réseaux inter-urbains (WAN) nationaux.

- Mise au rebut : pour tout départ définitif d'un matériel ou logiciel du service, le titulaire doit empêcher de manière sécurisée l'accès aux données présentes sur les disques durs ou dans la mémoire intégrée. Un procès-verbal doit être signé entre le titulaire et l'acheteur.

  En cas d'impossibilité de réaliser un effacement sécurisé sur tout ou partie des disques ou de la mémoire (par exemple pour raison de panne ou dysfonctionnement), le disque dur ou la mémoire doit être détruit(e) physiquement avant de quitter définitivement le service ou démonté(e) et entreposé(e) sur site dans un local sécurisé en attente de destruction.

Annexes

1. Les principaux documents applicables

Les documents internes de l'acheteur

Exemples : la PSSI de l'acheteur, le dossier d'homologation d'un système d'information

Les documents externes

Les documents suivants (*liste non exhaustive)* accessibles à partir du site de l'Agence Nationale de Sécurité des Systèmes d'information (ANSSI), dans leur version à leur date de publication, peuvent servir de référence dans la rédaction des contrats de l'acheteur :

Réglementation

- L'instruction interministérielle N°901 relative aux mesures de protection des systèmes d'information traitant d'informations sensibles non-classifiées de défense de niveau Diffusion Restreinte (DR)
  http://www.ssi.gouv.fr/administration/reglementation/protection-des-systemes-informations/instruction-interministerielle-n-901/
- L'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale *http://www.ssi.gouv.fr/administration/reglementation/protection-des-systemes-informations/instruction-generale-interministerielle-n-1300-sur-la-protection-du-secret-de-la-defense-nationale/*
- La Politique de Sécurité des Systèmes d'Information de l'État (PSSIE) *http://www.ssi.gouv.fr/administration/reglementation/protection-des-systemes-informations/la-politique-de-securite-des-systemes-dinformation-de-letat-pssie/*
- Le référentiel général de sécurité (RGS V2)
  http://www.ssi.gouv.fr/administration/reglementation/administration-electronique/le-referentiel-general-de-securite-rgs/

Guides

- Le guide « Maîtriser les risques de l'infogérance »
  http://www.ssi.gouv.fr/IMG/pdf/2010-12-03_Guide_externalisation.pdf
- Les recommandations et bonnes pratiques associées aux sujets ci-dessous :
  http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/
  - Authentification et mécanismes cryptographiques ;
  - Sécurité du poste de travail et des serveurs ;
  - Sécurité de la messagerie ;

- Sécurité des médias amovibles ;
- Sécurité des liaisons sans fil ;
- Sécurité des copieurs ou imprimantes multifonctions ;
- Sécurité des solutions de mobilité ;
- Sécurité des réseaux ;
- Sécurité des applications WEB ;
- Sécurité de l'externalisation ;
- Réaction en cas d'incident ;
- Sécurité des systèmes industriels.

  (Liste non exhaustive)

- Les guides de bonnes pratiques de la CNIL pour la protection des données à caractère personnel *http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_securite-VD.pdf*

- Le guide **«Achats informatiques et propriété intellectuelle »** élaboré de manière conjointe par l'APIE, la Direction interministérielle des systèmes d'information et de communication de l'État (DINSIC) et la Direction des achats de l'État (DAE)

2. Modèle de formulaire d'engagement et de déclaration de connaissance des règles de discrétion, de confidentialité et de sécurité informatique

ENGAGEMENT DE RECONNAISSANCE DE RESPONSABILITE

Relatif au respect des obligations de confidentialité, de protection des données à caractère personnel ou sensibles et des mesures de sécurité en vigueur à [entité]

***LA PERSONNE DESIGNEE CI-APRES* :**

NOM – Prénom :			
Né(e) le :		**à :**	
déclarant avoir toute autorité pour agir en tant que (*fonctions dans l'entreprise*) :			
au nom de la société désignée ci-contre *(raison sociale et adresse du siège social) :*			

dans le cadre de l'exécution du marché public xxx,

Reconnaît avoir été sensibilisée et de ce fait avoir pleinement connaissance :

- que l'autorisation d'accès aux locaux de l'acheteur est conditionnée à l'obtention d'une autorisation d'accès délivrée après enquête diligentée par le service de sécurité compétent, ce droit d'accès est strictement personnel, incessible et limité dans le temps ;
- que toute éventuelle action contraire aux règles édictées doit être immédiatement signalée à la [mettre le nom de la direction] et à sa voie fonctionnelle SSI ;
- que l'acheteur peut, à tout instant, demander à en contrôler sans restriction l'utilisation qui en est faite ;
- des dispositions générales relatives à la réglementation et à la législation française en vigueur dans le domaine de la sécurité des systèmes d'information et plus particulièrement à la fraude informatique, notamment les articles 323-1 à 323-3-1 du code pénal ;
- des dispositions de l'instruction interministérielle n°901 sur la protection des systèmes d'information sensibles ;
- des dispositions des articles 413-9 à 413-12 du code pénal relatifs aux atteintes au secret de la défense nationale ;
- des dispositions de l'arrêté du 30 novembre 2011 portant approbation de l'instruction générale interministérielle n°1300 sur la protection du secret de la défense nationale ;
- qu'un dispositif (journalisation des notifications techniques et de sécurité) permet d'assurer la traçabilité de l'ensemble des actions menées sur le système d'information, pour raisons de sécurité.

M'engage à ce que tous les agents appelés, sous ma responsabilité, à intervenir à un titre quelconque dans le cadre de l'exécution du marché :

- respectent l'obligation de discrétion professionnelle pour tous les faits, informations ou documents dont ils auraient connaissance dans l'exercice ou à l'occasion de l'exercice de leurs activités ;
- ne divulguent en aucun cas à un tiers des informations ou données tant personnelles que professionnelles qu'ils pourraient être amenés à apprendre dans l'exercice de leur mission ;
- ne reproduisent, ni ne stockent, ni ne copient, ni ne diffusent, ni ne modifient, ni n'altèrent, ni ne détruisent toute information ou donnée dont ils pourraient avoir connaissance à d'autres fins que celles de l'exercice de leur mission ;
- respectent le principe fondamental du « besoin d'en connaître » et ainsi ne tentent pas d'accéder, ni de reproduire, ni de stocker, ni de copier, ni de diffuser, ni de modifier, ni d'altérer, ni de détruire toute information dont ils ne sont pas supposés avoir connaissance dans l'exercice de leur mission.

M'engage à ce que tous les agents disposant d'un accès à un système d'information de l'administration et, par conséquent, d'un compte nominatif :

- ne tentent pas de connecter tout appareil électronique communicant ou non, personnel ou de la société, au système d'information sans avoir reçu préalablement l'autorisation formelle de la voie fonctionnelle SSI ;
- ne modifient pas sans autorisation la configuration des moyens mis à leur disposition et notamment ne raccordent pas de moyens informatiques qui n'auront pas été convenus au préalable avec l'acheteur dans le cadre de la définition de l'architecture ;
- ne se livrent pas à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des services, applications et moyens auxquels ils ont accès ;

- ne mettent pas à la disposition d'utilisateurs non autorisés un accès privilégié aux ressources informatiques, données ou services ;
- ne perturbent ni n'interrompent le fonctionnement normal du système d'information ou de l'un de ses composants ;
- n'installent pas, sans autorisation préalable et formelle de la voie fonctionnelle SSI (ou de son représentant) de logiciels sur le système d'information ou sur les équipements mis à leur disposition ;
- n'introduisent, ni ne testent, ni n'utilisent des supports informatiques ou médias dont l'origine leur est inconnue, douteuse ou incertaine ;
- ne génèrent pas volontairement ou involontairement des perturbations sur les ressources du SI que ce soit par des manipulations anormales ou par l'introduction illicite de logiciels contrefaits ou piratés potentiellement nuisibles en termes de failles de sécurité ou de pollution virale.

Déclare être pleinement consciente de mes responsabilités et reconnait être informée des conséquences pénales et contractuelles qui pourraient résulter de la non application des procédures et dispositions édictées ci-dessus.

A		le	
Recopier ci-dessous la formule manuscrite suivante : « ***je m'engage*** »			
CACHET DU TITULAIRE		**SIGNATURE DU TITULAIRE**	