# Annexe i : Protection des informations – Confidentialité – Mesures de sécurité

Dans la présente annexe, les dispositions relatives aux sous-traitants ne valent que dans  
les cas où la sous-traitance est autorisée par le marché. De la même façon, les dispositions relatives au support ou à la maintenance ne valent que si ces prestations sont prévues au marché.

## Référence au CCAG

Le titulaire est tenu de respecter les obligations de confidentialité, de protection des données à caractère personnel et les mesures de sécurité prévues à l’article 5 du CCAG applicable au marché contractualisé.

Si un sous-traitant est susceptible d'intervenir pour le compte du titulaire durant l'exécution de l’accord-cadre, le titulaire est tenu de l'aviser de ce que ces obligations lui sont applicables.

Quel que puisse être le statut de ce sous-traitant vis-à-vis du titulaire, ce dernier reste responsable du respect de ces obligations.

## Mesures de sécurité

### Mesures de sécurité

Le commandement du Service militaire adapté ou les régiments du SMA peuvent retirer son agrément à tout moment sans avoir à énoncer ses motifs, le titulaire doit alors proposer immédiatement un remplaçant de niveau équivalent.

### Mesures de sécurité applicables à l’accès aux locaux

Tout agent du titulaire, que celui-ci soit l'un de ses salariés ou salarié d'un de ses sous-traitants, devant avoir accès aux locaux de l'administration doit être préalablement nommément agréé selon la procédure en vigueur au Commandement du Service militaire adapté ou au régiment du Service militaire adapté (SMA) concerné.

Cet agent du titulaire demeure soumis pendant son séjour aux mêmes règles intérieures que les agents de l’administration, notamment les politiques et procédures de sécurité des systèmes d’information, ainsi que les chartes administrateurs et utilisateurs.

L'intervention dans les locaux de l'administration est conditionnée à l'obtention d'une autorisation d'accès délivrée à l'agent du titulaire après enquête diligentée par le service de sécurité compétent pour l'autorité contractante au profit de laquelle le marché est exécuté.

Le délai d'enquête est en moyenne de quinze (15) jours ouvrés et il est fait  
obligation au titulaire de fournir à l'administration :

* le patronyme et les prénoms de son agent ;
* une photocopie lisible et recto-verso d’un titre d’identité dont la nature varie selon la situation individuelle de l’agent visé :
  + carte nationale d’identité (CNI) ou passeport en cours de validité pour les ressortissants français et communautaires ;
  + titre de séjour en cours de validité avec autorisation de travail préalable ou carte de résident pour les étrangers extracommunautaires ;
* l’adresse actuelle de l’agent si celle-ci diffère de celle portée sur le titre d’identité fourni.

### Mesures de sécurité applicables à l’accès aux ressources de l’administration

Dès notification du marché et avant tout commencement d'exécution de celui-ci, le titulaire a obligation de remettre à l’administration l’engagement de reconnaissance de responsabilité signé (joint en annexe II au CCAP) en sa qualité de titulaire.

En cas de sous-traitance, acceptée préalablement par l’administration, le titulaire du marché s’engage à remettre un engagement de reconnaissance de responsabilité signé par le sous-traitant.

En cours d’exécution du marché, le titulaire a obligation de communiquer à l’administration la liste actualisée de ses agents, que ceux-ci soient salariés du titulaire ou salariés d'un de ses sous-traitants, susceptibles d'intervenir dans son exécution (ci-après désignée par la « Liste »).

L’actualisation de la Liste a lieu au minimum une fois par an, à la date anniversaire de la signature du marché.

Un original de l’engagement de reconnaissance de responsabilité est remis au responsable du projet de l’administration, ainsi qu’à l’interlocuteur du commandement ou du régiment du Service militaire adapté qui sera indiqué après la notification du marché.

La « Liste » doit être transmise au responsable du projet de l’administration, ainsi qu’à l’interlocuteur du régiment qui sera indiqué après la notification du marché.

Le titulaire s'engage à prendre toutes les mesures nécessaires et conformes à l’état de l’art en matière de sécurité des systèmes d’information pour assurer, lors de l'exécution du marché, la protection effective et efficace des informations ou supports qui peuvent être détenus dans le service, au profit duquel le marché est exécuté, ou dans tout lieu où ce marché est exécuté.

Le titulaire veille à sensibiliser ses personnels sur la nature et la sensibilité des informations et données communiquées par les agents du ministère de l’intérieur aux services supports. Il s’agit de s’assurer que dans le cadre de la résolution d’un incident ne sont communiquées ni données métiers ni données techniques (adresses IP, configuration d’équipement de sécurité [règles et exceptions]). S’il venait à être indispensable de détenir de telles informations, la communication entre les deux parties devra être effectuée au moyen d’un outil de chiffrement homologué par l’ANSSI et validé par l’administration. Le cas échéant, cet outil de chiffrement peut être fourni par l’administration.

Le titulaire reconnaît avoir pris connaissance, pour tous les agents appelés sous sa responsabilité à intervenir à un titre quelconque dans le cadre de l'exécution du marché, des articles 413-9 à 413-12 du code pénal et des dispositions de l'arrêté du 30 novembre 2011 portant approbation de l’instruction générale interministérielle (IGI) n°1300 sur la protection du secret de la défense nationale, et d’autre part, qu'ils n'ont pas, sous peine de poursuite pénale, à connaître ou détenir des informations couvertes par le secret de la défense nationale.

Aucune dérogation aux présentes mesures de sécurité ne pourra être acceptée de l'autorité contractante ou exigée d'elle, y compris en vue de pourvoir au remplacement inopiné, fortuit ou même urgent d'un agent du titulaire.

Le non-respect ou l’inobservation par le titulaire de ces mesures de sécurité, même dans  
les cas où ils résultent d'une imprudence ou d'une négligence, peuvent entraîner le  
prononcé d’une sanction contractuelle, sans préjudice des sanctions pénales.

## Protection des informations sensibles

### Principes

Toute information sensible du régiment doit être considérée comme un bien à protéger et ce tout au long de son cycle de vie.

Les niveaux de sensibilité des informations sont définis dans le tableau ci-après.

|  |  |
| --- | --- |
| **Niveau de sensibilité** | **Définition** |
| **Non sensible** | Données ou informations pouvant être diffusées volontairement ou dont la diffusion involontaire à l’extérieur du ministère ne porte pas de préjudice pour lui, ses partenaires du service public ou privés. |
| **Sensible** | Données ou informations ne devant pas être rendues publiques et/ou restreintes à la diffusion d’un domaine spécifique. |
| **Sensible « Diffusion Restreinte »** | Données ou informations soumises à une restriction de diffusion particulière. La « diffusion restreinte » relève de la nécessité d'éviter la divulgation, dans le domaine public, d'informations dont le regroupement ou l'exploitation pourraient :   * conduire à la découverte d’une information classifiée ; * porter atteinte à la sécurité ou à l’ordre public, au renom des institutions, à la vie privée de leurs membres ; * porter préjudice aux intérêts économiques ou financiers de sociétés privées ou d’établissements publics. |

Le titulaire s'engage à ce que les informations sensibles, pendant tout leur cycle de vie, ne  
puissent être portées, même fortuitement, à la connaissance de personnes n'ayant pas le  
besoin d'en connaître sauf accord préalable exprès et écrit de l’administration.

Dans les locaux du prestataire, les informations sensibles font l'objet d'une gestion spécifique.

Des informations sensibles peuvent se voir attribuer une protection par un marquage  
« Diffusion Restreinte » selon les règles posées par l'annexe 3 de l’IGI 1300. Les informations « Diffusion Restreinte » sont déterminées en fonction de la nature de la prestation et du type de données à protéger dans le marché.

Les informations sensibles considérées « Diffusion Restreinte » sont marquées avec la mention « Diffusion Restreinte » conformément au modèle ci-dessous :

**DIFFUSION RESTREINTE**

Pour les documents papier, cette mention « Diffusion Restreinte » est portée en haut de toutes les pages du document. Les informations techniques au format électronique, ne pouvant donc faire l’objet d’un marquage réglementaire comme indiqué ci-dessus (comme par exemple les journaux d’évènements, les fichiers de configuration, les codes sources), sont de facto considérées comme « Diffusion Restreinte » et le titulaire a l'obligation d'appliquer les dispositions réglementaires qui s’imposent pour la gestion de ces données.

La réalisation d'une copie d’une information considérée « Diffusion Restreinte » sans autorisation préalable est considérée par l’administration comme une violation des dispositions relatives au respect du secret dans l'exécution du marché.

### Protection des informations sensibles sur support papier

Le titulaire a l'obligation de mettre en place un système de gestion permettant d'identifier tous les documents comportant des informations sensibles, quel que soit leur marquage, et pour chacun de ces documents ainsi identifié :

* de connaître la liste des personnes physiques comme morales en ayant eu connaissance ou communication ;
* d'en connaître soit la date de restitution à l'administration soit la date de destruction, ainsi que le nom et la qualité de la personne ayant réalisé l'opération.

En cas de destruction, un bordereau de destruction doit être établi par le titulaire qui identifie le ou les documents détruits, le ou les agents du titulaire ayant procédé à la destruction, le ou les agents du titulaire ayant assisté à la destruction en qualité de témoin(s), et le moyen de destruction utilisé (broyage ou incinération). Ce bordereau est transmis, sans délai, à l’interlocuteur désigné issu du commandement ou du régiment.

Le bordereau de destruction stipule que le titulaire certifie n'avoir ni établi ni conservé de copie des informations sensibles.

En cas de restitution, un bordereau de restitution doit être établi par le titulaire qui identifie le représentant de l'administration à qui est remis le document. Au surplus, le bordereau doit stipuler que le titulaire certifie n'avoir ni établi ni conservé de copie du document.

La diffusion des documents papier se fait sous double enveloppe. L’enveloppe extérieure ne porte aucune mention particulière hormis le nom et l'adresse du destinataire. L'enveloppe interne porte le nom du destinataire et la mention pertinente, à savoir « Sensible » ou « Diffusion Restreinte ». Les agents du titulaire qui gèrent les arrivées courrier doivent être sensibilisés à l’usage de ces mentions, ne pas ouvrir l’enveloppe et la distribuer au destinataire.

### Protection des informations sensibles sur support électronique

Il est fait obligation au titulaire que le traitement des informations sensibles sur support  
électronique ne soit pas réalisé sur des moyens informatiques connectés à un réseau non  
maîtrisé. L'administration considère qu'un réseau d'entreprise connecté à Internet ne  
permet pas de garantir ce niveau adéquat de protection des informations sensibles.

Le cas échéant, le titulaire peut s'efforcer de démontrer à l'administration son aptitude à  
protéger les informations sensibles qu'il serait amené à traiter en dehors des systèmes d'information du ministère de l'intérieur. Pour ce faire :

* soit l'isolation des moyens de traitement des informations s'effectue de manière physique ;
* soit cette isolation s'effectue par une interface logique de sécurité présentant des garanties suffisantes afin d'empêcher l'accès aux moyens de traitement des informations sensibles par des tiers.

Le titulaire doit alors soumettre à l'administration une documentation relative aux règles de gestion et aux règles techniques de sécurité de ces moyens de traitement des informations sensibles. Ces règles de gestion et règles techniques de fonctionnement concourant à la sécurité des informations sensibles doivent faire l'objet d'une validation formelle par l'administration. Cette dernière se réserve le droit de procéder à leur contrôle préalablement à toute validation comme après validation pendant l'exécution du marché.

Il est fait obligation au titulaire de respecter le besoin d'en connaître : seuls ses agents de la Liste ont accès aux informations nécessaires pour l’exécution du marché. Le respect de cette obligation par le titulaire doit être garanti par la mise en place et l'utilisation de mécanismes de sécurité (authentification individuelle, gestion des droits et traçabilité des accès).

La confidentialité des informations sensibles, quel que soit leur marquage, sur support électronique est réalisée au moyen d'un mécanisme de chiffrement reposant sur un logiciel « qualifié » par l'agence nationale de la sécurité des systèmes d’information (ANSSI). Ces logiciels sont fournis par l’administration dès notification du marché. Un document relatif à l’utilisation de ces logiciels est remis au titulaire dès notification du marché, il doit faire l'objet d'une diffusion auprès de ses agents intervenant dans le cadre des prestations prévues.

A l’issue du marché, le titulaire procède soit à la restitution, soit à la destruction de l’ensemble des informations sensibles sur support électronique et des documents associés incluant les courriels :

* en cas de restitution, un bordereau de restitution doit être établi par le titulaire qui identifie le représentant de l'administration à qui sont remis les informations sensibles sur support électronique, en déclare la liste et stipule que le titulaire certifie n'avoir ni établi ni conservé de copie des informations sensibles ;
* en cas de destruction, un bordereau de destruction doit être établi par le titulaire qui identifie les supports électroniques détruits, le ou les agents du titulaire ayant procédé à la destruction, le ou les agents du titulaire ayant assisté à la destruction en qualité de témoin(s), le ou les moyens de destruction utilisés. Ce bordereau est transmis, sans délai, à l’interlocuteur désigné issu du commandement ou du régiment.

Le bordereau de destruction stipule que le titulaire certifie n'avoir ni établi ni conservé de copie des informations sensibles. Le mécanisme de destruction utilisé doit reposer sur un outil « qualifié » par l’ANSSI. Le cas échéant, cet outil est fourni par l’administration.

### Sécurisation des locaux du titulaire

Dans le cas où des informations sensibles, quel que soit leur marquage et quelle que soit  
la forme de leur support, sont appelées à être conservées dans les locaux du titulaire, leur  
support papier ou électronique doivent être disposés en dehors de leur utilisation dans des  
armoires fermant à clé et dont la clé est conservée par la seule personne responsable de leur utilisation.

Préalablement à toute exécution du marché, le titulaire doit désigner un responsable sécurité qui devient l'interlocuteur privilégié de l'administration pour tous les sujets de sécurité pendant l'exécution du marché.

Il appartient à ce responsable sécurité de sensibiliser les agents du titulaire susceptibles d’intervenir dans l’exécution du marché au strict respect des obligations du titulaire en matière de SSI et d'en présenter un bilan à l'occasion de la réunion du comité de suivi ou de toute instance équivalente prévus dans les documents du marché.

### Modalités d’exécution

A tout moment pendant l'exécution du marché, l’administration se réserve le droit de réaliser tout contrôle, après un préavis de vingt-quatre (24) heures, dans les locaux du titulaire pour vérifier que sont effectivement respectées les préconisations validées par l'administration s'agissant des règles de gestion et des mesures techniques de sécurisation des moyens de traitement des informations sensibles du ministère de l’intérieur.

En cas de défaillance constatée dans la mise en œuvre de mesures de sécurité en adéquation avec le niveau de sensibilité des données traitées, il pourra être fait obligation au titulaire de réaliser à ses frais tous travaux de mise en conformité de ses locaux.

Le titulaire a le devoir d’informer sans délai l’administration de toute difficulté dans l’application de ces mesures, de fuite ou de suspicion de fuite d’informations sensibles qu’il rencontre ou constate.

### Obligation de respect déontologique

Les intervenants des titulaires réalisent leurs prestations avec probité et intégrité.

Ils veillent à prévenir ou à faire cesser immédiatement tout conflit d’intérêts, défini comme une situation d’interférence entre un intérêt public et des intérêts publics ou privés qui est de nature à influencer ou à paraître influencer l’exercice indépendant, impartial et objectif de leur profession.

Les titulaires et les bénéficiaires s’engagent à respecter toutes les mesures déontologiques applicables dans le cadre de l’exécution des prestations.

Les intervenants doivent être à jour de leurs obligations déontologiques, notamment pour les anciens agents publics (autorisation de la commission de déontologique de l’administration d’origine ou autorisation de l’employeur soumise à approbation de l’administration bénéficiaire). Au-delà des poursuites pénales applicables, l’administration peut être amenée à écarter du suivi du présent accord-cadre toute personne (titulaire ou bénéficiaire) ne respectant pas ces règles.

Avant chaque mission, le titulaire, co-traitant ou sous-traitant complète l’annexe du CCAP certifiant l’absence de conflit d’intérêt ou identifiant les potentiels conflits existants. Elle est communiquée à l’administration sans délai, pour tous les membres de l’équipe mobilisée pour la réalisation des prestations. L’annexe est également complétée par l’entreprise en tant que personne morale. Cette déclaration est complétée quel que soit le statut de l’entreprise mobilisée : mandataire, co-traitant, sous-traitant. L’administration bénéficiaire pourra statuer sur les déclarations transmises et prendre les mesures idoines afin de faire cesser tout conflit d’intérêt (demande de remplacement, mise en impossibilité d’honorer la commande, etc.).

En cas de modification substantielle des intérêts détenus au cours de la prestation, le prestataire et les consultants actualisent leur déclaration dans un délai de quinze jours et selon les mêmes modalités.

Tout au long de l’exécution de l’accord-cadre, le titulaire est tenu de déclarer sous sa responsabilité, à l’acheteur toute situation de nature à constituer un conflit d’intérêts.

Les titulaires s’engagent à ne pas proposer aux agents publics des récompenses de nature qui auraient pour conséquence le non-respect des principes déontologiques. Sont ainsi proscrits les comportements, actifs ou passifs, visant à bénéficier ou faire bénéficier d’un avantage quelconque par le biais de récompense en nature (repas, invitation hors cadre professionnel, cadeaux individuels, etc.). Toute action de démarchage ou invitation à des évènements promotionnels de la part du titulaire auprès des bénéficiaires est prohibée.

### Mesures de sécurité, dont sécurité informatique et gestion des données

Toute personne relevant du titulaire ou de ses sous-traitants est soumise, le cas échéant, à des mesures de sécurité qu’il s’agisse d’accès physiques à des locaux ou d’accès logistiques à des informations.

Le titulaire doit faire connaître à l’acheteur, sur la demande de ce dernier, le lieu d’exécution des prestations.

Afin de se prémunir contre toute insuffisance de protection du lieu d’exécution, l’acheteur peut effectuer ou faire effectuer un audit de sécurité auprès d’un ou plusieurs titulaires (ou de ses/leurs sous-traitants) afin de s’assurer de la prise en compte effective du niveau de sécurité requis par lui/eux. Le titulaire/Les titulaires doit/doivent être informé(s) quinze jours à l’avance de cet audit (date, modalités de mise en œuvre). Ce contrôle peut durer pendant une période de six mois au-delà de la résiliation ou de la fin de l’accord-cadre, afin de vérifier que l’ancien titulaire a pris les dispositions en matière de destruction des données.

Destruction et restitution des informations collectées par le titulaire : Le titulaire garantit la destruction des données utilisées dans le cadre de la réalisation des prestations après restitution de ces dernières à l’administration. Au terme de l’exécution 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 détruit, sans délai et définitivement 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 sont constatées par un procès-verbal daté et signé par le titulaire. Les procédés de destruction sont conformes aux réglementations en vigueur.

### Mise en place de l’équipe technique

Les titulaires s’engagent à mettre en place et maintenir, pendant toute la durée de l’accord-cadre, des intervenants dont les profils et compétences doivent impérativement respecter ceux mentionnés dans la composition de l’équipe affectée à la prestation (représentants du titulaire et son équipe) laquelle figure son offre technique conformément aux compétences attendues dans le CCTP.

Le titulaire communique à l’administration, à sa demande, l’identité, les titres, le curriculum vitae et les coordonnées professionnelles des personnes physiques en charge de l’exécution des prestations.

### Identification du titulaire

Dans le cadre de l’exécution des prestations, il est primordial qu’aucun doute ne soit entretenu concernant la qualité de prestataire du titulaire, tant en interne que vis-à-vis des tiers.

Les membres de l’équipe mobilisés sont tenus d’indiquer leur identité ainsi que le nom de l’entreprise qui les emploie dans leurs contacts avec l’administration bénéficiaire et les tiers avec qui ils échangent pour les besoins de leurs prestations (signature de courriel, présentation en réunion, etc.).

### Remplacement des intervenants

Lors de l’exécution des prestations, le titulaire maintient les profils de l’équipe dédiée telle que définis au stade de la passation des commandes ou de la conclusion d’un marché subséquent.

Le service bénéficiaire de l’accord-cadre se réserve le droit de demander le remplacement motivé d’un ou de plusieurs intervenants du titulaire. De même, en cas de départ, le titulaire doit :

* En aviser, sans délai, le bénéficiaire et prendre toutes dispositions nécessaires afin d’assurer la poursuite de l’exécution des prestations ;
* Proposer au bénéficiaire un remplaçant disposant de compétences au moins équivalentes. Il en communique l’identité, les titres, le curriculum vitae et les coordonnées professionnelles dans un délai de 5 jours calendaires à compter de la date d’envoi de l’avis mentionné à l’alinéa précédent.

Pendant la période de carence, le titulaire désigne un interlocuteur temporaire ayant une bonne connaissance des prestations.

En cas de changement d’un intervenant à l’initiative du titulaire, la période minimale de recouvrement pendant laquelle le partant communique à son successeur toutes les informations relatives au projet est fixée à 10 jours calendaires.

Par dérogation à l’article 3.4.3 du CCAG-PI, le remplaçant proposé par le titulaire est considéré comme accepté par le bénéficiaire si celui-ci ne récuse pas dans un délai de 15 jours. Si le bénéficiaire récuse le remplaçant, le titulaire dispose de 10 jours pour proposer d’autres remplaçants. La décision de récusation prise par le bénéficiaire est motivée.

Les avis, propositions et décisions du bénéficiaire sont notifiés selon les modalités fixées à l’article 3.1 du CCAG-PI. A défaut de proposition d’au moins un remplaçant par le titulaire ou en cas de récusation des remplaçants par le bénéficiaire, il peut être mis fin à l’exécution de la commande ou le marché subséquent peut être résilié.

En aucun cas, le remplacement du personnel ne pourra justifier une augmentation du montant des prestations.

### Exigences relatives aux prestations

Le service bénéficiaire s’engage à mettre à disposition du titulaire les informations en sa possession nécessaires pour mener à bien les prestations décrites dans le CCTP.

Le titulaire est responsable de tout élément qui lui est confié. Il ne peut en disposer qu’aux fins prévues par l’accord-cadre. Il est notamment responsable de la conservation, de l’entretien et de l’emploi et de tout matériel, objet, données numériques ou approvisionnement qui lui est confié dès que ce matériel, objet, données numériques ou approvisionnement est mis effectivement à sa disposition. Il ne peut en disposer qu’aux fins prévues par le présent accord-cadre.

Le titulaire applique et fait appliquer à ses sous-traitants éventuels les clauses de sécurité du présent accord-cadre.

### Communication entre les parties

Les parties se transmettent les informations, décisions et documents relatifs à l’exécution de l’accord-cadre par tout moyen de communication permettant de déterminer de façon certaine la date et l’heure de réception.

L’administration peut refuser la communication d’informations, notamment au regard des impératifs de sécurité et de confidentialité, par décision dûment motivée, notamment pour des raisons de confidentialité ou si elle considère que cette demande n’est pas en rapport ou n’est pas nécessaire à la réalisation de la prestation commandée.

Le titulaire ne peut se prévaloir d’une insuffisance d’informations pour se décharger de sa responsabilité, sauf à démontrer un lien suffisamment direct entre un refus de communication et un manquement de sa part.

Les informations sont échangées dans le respect du règlement général sur la protection des données. Le titulaire répond à toute demande d’information ou de transmission de documents en rapport avec l’exécution du présent accord-cadre.