ANNEXE I : PROTECTION DES INFORMATIONS – CONFIDENTIALITE – MESURES DE SECURITE

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.

1. 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.

2. Mesures de sécurité

2.1 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 ministère de l'intérieur (MI). 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. Le ministère de l'intérieur peut retirer son agrément à tout moment sans avoir à énoncer ses motifs, le titulaire doit alors proposer immédiatement un remplaçant de niveau équivalent.

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 une autorisation de travail valable 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.

2.2 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'officier de sécurité (OS) du pôle SSI, à l'adresse suivante :

Pôle SSI
Immeuble Lumière
40, Avenue des Terroirs de France
75 012 PARIS

La Liste doit être transmise au responsable du projet de l'administration, ainsi qu'à l'officier de sécurité du pôle SSI à l'adresse suivante :

dsic-poleSSI@interieur.gouv.fr

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 323-1 à 323-3-1 et 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.

3. Protection des informations sensibles

3.1. Principes

Toute information sensible du ministère de l’intérieur 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.

La politique de sécurité des systèmes d’information (PSSI) du ministère de l'intérieur (PSSI-MI), comme la PSSI pertinente pour le service au profit duquel le marché est exécuté, sont réputées connues du titulaire comme de ses agents de la Liste qu’il aura déclarée à l’administration. Le titulaire s’engage à respecter, et faire respecter par ses agents, l'ensemble des obligations de ces PSSI.

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. Sont notamment systématiquement considérés comme « Diffusion Restreinte » :

- les plans d'adressage IP du ministère (ou une partie de ces plages si cela permet de cartographier un sous-ensemble du système d'information) ;
- les mots de passe ;
- les fichiers de configuration ;
- les codes sources des applications (ou un extrait de ces codes sources) ;
- les fiches d'expression rationnelle des objectifs de sécurité (FEROS) et dossiers d'analyse de risques ;
- les dossiers de sécurité des systèmes d'information du ministère de l'intérieur, que ces systèmes soient en mode projet ou en mode opérationnel ;
- les dossiers d'architecture et d'installation ;
- les données de production.

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.

3.2. 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'officier de sécurité du PSSI, à l'adresse suivante :

dsic-poleSSI@interieur.gouv.fr

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.

3.3. 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[1] : seuls ses agents de la Liste ont accès aux informations nécessaires pour l'exécution du marché. Le respect de

[1] Le besoin d'en connaître désigne la nécessité impérieuse de prendre connaissance d'une information dans le cadre d'une fonction déterminée et pour la bonne exécution d'une mission précise.

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'officier de sécurité du pôle SSI (PSSI), à l'adresse suivante :

  dsic-poleSSI@interieur.gouv.fr

  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.

3.4. 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. L'administration se réserve le droit de vérifier le niveau de compétences en sécurité des systèmes d'information (SSI) de ce responsable et de le récuser si elle juge ce niveau insuffisant, le titulaire ayant alors l'obligation de proposer sans délai à l'administration un nouveau responsable sécurité.

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.

3.5. 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.

4. Glossaire

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
DSIC	Direction des Systèmes d'Information et de Communication du ministère de l'intérieur
FEROS	Fiche d'Expression Rationnelle des Objectifs de Sécurité
IGI	Instruction Générale Interministérielle
IP	Internet Protocol
MI	Ministère de l'Intérieur
PSSI	Politique de Sécurité des Systèmes d'Information
PSSI-MI	Politique de Sécurité des Systèmes d'Information du Ministère de l'Intérieur
PES	Procédure d'Exploitation de la Sécurité des Systèmes d'Information
RCSSI	Responsable Central de la Sécurité des Systèmes d'Information
RGSSI	Responsable Général de la Sécurité des Systèmes d'Information
RSSI	Responsable de la Sécurité des Systèmes d'Information
RSSI-E	Responsable de la Sécurité des Systèmes d'Information « Expertise »
RSSI-H	Responsable de la Sécurité des Systèmes d'Information « Homologation »
RSSI-TU	Responsable de la Sécurité des Systèmes d'Information « Terminal utilisateurs »
OS	Officier Sécurité
SI	Système d'Information
SSI	Sécurité des Systèmes d'Information
SSMI	Service de Sécurité du Ministère de l'Intérieur
Pôle SSI	Pôle Sécurité des Systèmes d'Information