

MEAE_23069_DIL

« Prestations **d'AMO BIM et BIM manager pour le projet ERA** »

ANNEXE 2 au CCAP

CLAUSES DE SECURITE ET ENGAGEMENT DE CONFIDENTIALITE

DOCUMENT A RETOURNER SIGNE IMPERATIVEMENT **AVEC L'OFFRE DU CANDIDAT**

Le présent document précise les objectifs et les moyens mis en œuvre pour respecter les conditions de sûreté exigées par l'organisation et le fonctionnement du Quai d'Orsay.

Les documents, supports et informations traitant du projet ERA, sont considérés comme « informations sensibles » et peuvent faire **l'objet de la mention de protection** « Diffusion restreinte ».

Construction de ce document :

- Rappel des règles générales à retourner signé **dans l'offre.**
- ANNEXE 2.1 (déclaration individuelle) : A retourner au MOA tout au long de l'étude du DCE par le titulaire en fonction des personnes qui travaillent sur ce dossier
- ANNEXE 2.2 (socle de sécurité) : à retourner signé **dans l'offre.**

Les clauses de sûreté sont les suivantes :

- **les clauses de confidentialité de l'information**, les exigences de sécurité, et les clauses relatives au contrat sensibles, **applicables pour l'ensemble des documents supports et informations** traitant du projet.

CLAUSES RELATIVES AUX CONTRATS SENSIBLES

La société, ses salariés et ses éventuels sous-traitants s'engagent à ne pas divulguer sous quelque forme que ce soit des informations, renseignements, documents dont il a ou aurait pu avoir connaissance à



l'occasion de l'exécution des prestations prévues au titre du présent contrat et de ses éventuels avenants.

1-Liste nominative du personnel.

1-1 Avant le démarrage des prestations.

L'entreprise qui transmettra une offre s'engage à remettre au MEAE, avant le début d'exécution des prestations *une liste nominative du personnel affecté à l'exécution des prestations.*

1-2. Pendant l'exécution des prestations.

La société s'engage à tenir à jour la liste et à faire mention des modifications qui peuvent intervenir dans la composition du personnel.

2- Comportement du personnel

La société s'engage à ce que son personnel :



-  Fasse preuve de discrétion,
-  N'ait aucune activité ou attitude en inadéquation avec la nature de la prestation,

CLAUSE RELATIVES A LA PROTECTION DU SECRET OU DIFFUSION RESTREINTE

L'entreprise admise à remettre une offre **reconnait avoir pris connaissance de l'instruction générale interministérielle n°1300/SGDSN du 9 août 2021 sur la protection du secret de la défense nationale et de son décret n° 2019-1271 du 2 décembre 2019 relatif aux modalités de classification et de protection du secret de la défense nationale.**

La société reconnaît avoir pris connaissance des articles 413-9 à 413-12 du code pénal et qu'il n'a pas à connaître ou détenir les informations couvertes par le secret de la défense nationale.

La société doit faire signer par tous les personnels, appelés sous sa responsabilité à un titre quelconque à intervenir pour son compte pour exécuter les prestations (compris les études), une déclaration individuelle par laquelle lesdits personnels attestent :

-  Avoir pris connaissance des articles 413-9 à 413-12 du code pénal ;
-  Qu'ils n'ont pas, sous peine de poursuite pénale, à connaître ou détenir des informations couvertes par le secret de la défense nationale.

La société s'engage à ce que seules les personnes ayant préalablement souscrit la déclaration précitée peuvent prendre connaissance du DCE du projet ERA.

La société s'engage à remettre au MEAE les déclarations individuelles ci-dessus avant toute étude du DCE du projet ERA.

Aucune dérogation aux prescriptions ci-dessus ne pourra être acceptée de l'autorité contractante.

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



Clause protection secret

Consécutive au décret n° 2019-1271 du 2 décembre 2019 relatif aux modalités de classification et de protection du secret de la défense nationale, l'instruction générale interministérielle n° 1300/SGDSN/PSE/PSD du 9 août 2021 sur la protection du secret de la défense nationale (IGI 1300) détermine les rôles et responsabilités ainsi que les exigences liées à la gestion du cycle de vie d'une information ou d'un support classifié.

Le Titulaire du présent contrat reconnaît avoir pris connaissance de l'instruction générale interministérielle n° 1300/SGDSN/PSE/PSD du 9 août 2021 sur la protection du secret de la défense nationale ;

Le Titulaire s'engage à prendre toutes les mesures utiles pour assurer lors de l'exécution du contrat la protection absolue des informations ou supports classifiés qui peuvent être détenus dans tout lieu dans lequel ce contrat est exécuté ;

Le Titulaire reconnaît avoir pris connaissance des articles 413-9 à 413-12 du code pénal et qu'il n'a pas à connaître ou détenir les informations couvertes par le secret de la défense nationale ;

Le Titulaire doit faire signer par tous les personnels, appelés sous sa responsabilité à un titre quelconque à intervenir pour son compte pour exécuter les prestations, une déclaration individuelle par laquelle lesdits personnels attestent :

- avoir pris connaissance des articles 413-9 à 413-12 du code pénal ;

- qu'ils n'ont pas, sous peine de poursuite pénale, à connaître ou détenir des informations couvertes par le secret de la défense nationale.

Le Titulaire s'engage à ce que seules les personnes ayant préalablement souscrit la déclaration précitée accèdent au dossier.

Le Titulaire s'engage à remettre au MEAE les déclarations individuelles avant étude du dossier DCE.

Aucune dérogation aux prescriptions ci-dessus 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 personnel du Titulaire.

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

Les données contenues dans ces supports et documents sont strictement couvertes par le secret professionnel (article 226-13 du code pénal), il en va de même pour toutes les données dont la société prend connaissance à l'occasion de l'exécution du présent contrat.

Conformément à l'article 34 de la loi informatique et libertés modifiée, la société s'engage à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des personnes non autorisées.



La société s'engage donc à respecter les obligations suivantes et à les faire respecter par son personnel :

- 📁 Ne prendre aucune copie des documents et supports d'informations qui lui sont confiés, à l'exception de celles nécessaires à l'exécution de la présente prestation prévue au contrat, l'accord préalable du maître du fichier est nécessaire ;
- 📁 Ne pas utiliser les documents et informations traités à des fins autres que celles spécifiées au présent contrat ;
- 📁 Ne pas divulguer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales ;
- 📁 Prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d'exécution du contrat ;
- 📁 Prendre toutes mesures de sécurité, notamment matérielles, pour assurer la conservation et l'intégrité des documents et informations traités pendant la durée du présent contrat ;
- 📁 Et en fin de contrat, à procéder à la destruction de tous fichiers manuels ou informatisés stockant les informations saisies.

À ce titre, la société ne pourra sous-traiter l'exécution des prestations à une autre société, ni procéder à une cession de marché sans l'accord préalable du MEAE.

Le MEAE se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect des obligations précitées par le titulaire.

A.....

Le.....

Nom du représentant de la société :

Signature



ANNEXE 2.1

DECLARATION INDIVIDUELLE (pour chaque personnel)

A retourner signée via la Plate-forme des achats de l'Etat (PLACE) dans l'offre

Je soussigné (e) ,.....

De l'entreprise.....

Numéro du macro-lot.....

En qualité de

Déclare,

- ☒ Avoir pris connaissance de l'IGI 1300/SGDSN du 9 août 2021 et de son décret n°2019-1271 du 9 décembre 2019
- ☒ Avoir pris connaissance des articles 413-9 à 413-12 du code pénal ;
- ☒ Ne pas, sous peine de poursuite pénale, à connaître, à divulguer ou détenir des informations couvertes par le secret de la défense nationale.

A

Le

Nom et signature du déclarant.....

ANNEXE 2.2



ANNEXE 2.2

SOCLE DE SECURITE

A retourner signée via la Plate-forme des achats de l'Etat (PLACE) dans l'offre

Le socle de sécurité de base, défini ci-dessous, doit être considéré comme étant le minimum requis en termes de principes à suivre et de règles à appliquer dans la gestion des données informatiques nécessaires à l'exécution des prestations. Selon le niveau d'exposition d'un événement et la nature des menaces identifiées, ce socle de base peut être complété par des mesures spécifiques destinées réduire la probabilité d'occurrence et les impacts de ces menaces spécifiques.

Les principes directeurs de ce socle de sécurité sont les suivants :

- la maîtrise de l'information ;
- la maîtrise des accès ;
- la sauvegarde des données ;
- les mises à jour des logiciels utilisés ;
- autres dispositifs de protection.

La maîtrise de l'information passe par le respect des mesures suivantes :

- lorsqu'un ordinateur portable est utilisé, les informations doivent être chiffrées sur le disque à l'aide d'un dispositif de type BitLocker ou équivalent. Les clés USB et les disques amovibles utilisés doivent disposer d'un dispositif équivalent ;
- le recours à des espaces de stockage de documents sur le cloud est conditionné à des garanties de confidentialité équivalentes aux dispositifs de stockage ci-dessus ;
- les messageries utilisées doivent être des messageries d'entreprise, les messageries Gmail, Yahoo ou équivalent sont à proscrire. L'activation du protocole TLS 1.2 minimum est obligatoire. Un logiciel antivirus est également indispensable pour contrôler les messages ainsi que les pièces jointes.
- la diffusion des informations sensibles doit être limitée uniquement aux personnes ayant besoin d'en connaître.

La maîtrise des accès nécessite :

- l'existence d'une politique de gestion des accès décrite et appliquée ; des revues devront être réalisées régulièrement ;
- des mots de passe à 10 à 12 caractères aléatoires incluant majuscule, minuscule et caractères spéciaux, un changement des mots de passe tous les 3 mois ainsi que l'usage d'un coffre-fort de type KeePass ou équivalent ;



- le recours à une authentification multifacteur pour tout accès à des bases de données contenant des données sensibles et/ou un volume important de données à caractère personnel (Exemple : la base d'accréditation des participants, journalistes ou personnel technique ...) ;
- l'ensemble des mots de passe par défaut des logiciels utilisés doit être impérativement changé (Base de données, système d'exploitation, interface d'administration des équipements) par des mots de passe résistants aux attaques par force brute.

La sauvegarde des données :

- les sauvegardes doivent être réalisées régulièrement à la fréquence suffisante pour éviter des processus de re-saisie de données longs, exigeant des délais incompatibles avec le planning. La fréquence doit être élevée et les supports régulièrement testés. Les supports de sauvegarde utilisés doivent impérativement être stockés dans des locaux sécurisés différents afin de ne jamais perdre les contenus des postes de travail et les sauvegardes en même temps ;
- si les données sauvegardées contiennent des données à caractère personnel et/ou sensibles, alors les sauvegardes doivent être chiffrées ;
- la durée de conservation des données est nécessaire jusqu'à la décision, par le MEAE de l'entreprise qui sera retenu pour réaliser les marchés de travaux. Les entreprises qui ne seront pas retenues pour cette offre devront réaliser la destruction de l'ensemble des éléments relatifs au DCE et aux études de chiffrage le jour de la réception par l'entreprise de cette décision.

Les mises à jour des systèmes d'information :

- les systèmes d'exploitation des serveurs et des postes de travail doivent être régulièrement mis à jour, ainsi que les composants (base de données, serveur http, proxy et tout autre logiciel nécessaire au SI) ;
- les correctifs, liés à des failles de sécurité, diffusés par les éditeurs doivent être impérativement appliqués. Si un risque élevé de dysfonctionnement existe lors de l'application d'un correctif, le prestataire doit informer immédiatement la Maîtrise d'ouvrage et proposer des mesures compensatoires destinées à limiter fortement la probabilité et les impacts subis si la faille de sécurité était exploitée.

Autres dispositifs de protection :

- des pare-feux doivent être installés sur chaque poste de travail et sur les serveurs, aucun flux n'est autorisé par défaut, ils doivent être explicitement autorisés ;
- les accès Internet ne doivent en aucun cas être réalisés à partir d'un compte ayant un privilège Admin ;
- un accès VPN ne doit pas être utilisé en simultané avec un accès direct sur Internet depuis le poste de travail ;



- l'usage des clés USB doit être limité et le contenu contrôlé, l'utilisation d'une station blanche est recommandée pour s'assurer que les fichiers ne contiennent pas des virus ou autres malwares lorsque l'origine de la clé n'est pas maîtrisée.

A.....

Le.....

Nom du représentant de la société :

Signature

