



ENGAGEMENT DU SOUSMISSIONNAIRE EN MATIÈRE DE PROTECTION DE L'INFORMATION DE DIFFUSION RESTREINTE - DECLINAISON EN REGLES DE SÉCURITÉ INFORMATIQUE

SOMMAIRE

TERMINOLOGIE	2
ARTICLE 1 - OBJET	3
ARTICLE 2 - EXIGENCES DE SECURITE INFORMATIQUE	3
ARTICLE 3 - REGLES DE CONFIGURATION ET D'UTILISATION	4
3.1 PROTECTION DU SYSTEME INFORMATIQUE	4
3.2 SAUVEGARDES	4
3.3 SUPPORTS AMOVIBLES	4
ARTICLE 4 - COMMUNICATIONS PAR VOIE ELECTRONIQUE	5
4.1 PRINCIPES GENERAUX	5
4.2 MANIPULATION DES CONTENEURS CHIFFRES	5
4.3 POLITIQUE DES MOTS DE PASSE	5
ARTICLE 5 - FIN DE PROCEDURE - RESTITUTION	6
ARTICLE 6 - AUDIT ET CONTROLE	6
ARTICLE 7 - ENGAGEMENT DU SOUSMISSIONNAIRE	6

TERMINOLOGIE

ACID	Logiciel de chiffrement (générant des conteneurs chiffrés)
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CEA	Commissariat à l'Energie Atomique et aux énergies alternatives
DAM	Direction des Applications Militaires
DO	Diffusion Ordinaire (informations non protégées mais réservées à une diffusion interne au sein de l'entreprise)
DR	Diffusion Restreinte (définition de l'IGI 1300)
GSM	Global System for Mobile communications (connexion téléphonie mobile)
HFDS	Haut Fonctionnaire de Défense et de Sécurité
PPST	Protection du Patrimoine Scientifique et Technique
S	Secret (définition de l'IGI 1300)
SF	Spécial France (définition de l'IGI 1300)
SI	Système d'Information
SSI	Sécurité des Systèmes d'Information
TS	Très Secret (définition de l'IGI 1300)
USB	Universal Serial Bus
WIFI	Wireless Protocol Access (Accès réseau sans fil)
Zed	Logiciel de chiffrement de conteneurs
ZoneCentral	Logiciel de chiffrement (générant aussi des conteneurs chiffrés Zed)

ARTICLE 1 - OBJET

Le présent document précise les règles de sécurité informatique qui doivent être respectées par les soumissionnaires aux consultations menées par la Direction des applications militaires du Commissariat à l'Energie Atomique et aux énergies alternatives et donnant lieu à l'échange d'informations à caractère sensible, faisant l'objet d'une mention de protection particulière « diffusion restreinte » (DR) visant à garantir leur confidentialité.

Ce document doit être signé par un représentant du soumissionnaire ayant tout pouvoir à cet effet et être retourné avec les autres pièces du dossier de candidature.

En cas de candidature en groupement momentané d'entreprises, un exemplaire de ce document doit être établi et retourné par le mandataire ainsi que par chaque membre du groupement (cotraitant) concerné par l'échange d'information à caractère sensible.

De même, un exemplaire de ce document doit être rempli et retourné pour chaque sous-traitant du titulaire auquel il est envisagé de faire appel dans la phase d'élaboration de l'offre et concerné par l'échange d'information à caractère sensible.

Rappel : Le présent document traite des Systèmes d'Information (SI) utilisés par le soumissionnaire pour sa réponse à la consultation. Le soumissionnaire devra impérativement mentionner dans son offre, les systèmes d'information qui lui sont propres ou qu'il entend créer spécifiquement et utiliser dans le cadre de l'exécution du marché. Ces systèmes devront être conformes aux règles citées à l'article 2 auxquelles s'ajouteront les guides ANSSI « sur la maîtrise SSI des systèmes industriels » et les prescriptions spécifiques au marché.

ARTICLE 2 - EXIGENCES DE SECURITE INFORMATIQUE

La réponse à la consultation implique le traitement d'informations ou supports sensibles (DR).

Le soumissionnaire s'engage à traiter ces informations ou supports, portant la mention de protection DR, dans le respect des règles édictées par les dispositions légales et réglementaires en vigueur, l'Instruction Générale Interministérielle n°1300 du 13 novembre 2020 sur la protection du secret de la défense nationale (IGI 1300), l'Instruction Interministérielle relative à la protection des systèmes d'informations sensibles n° 901/SGDSN/ANSSI et, en conséquence, le guide ANSSI « Hygiène Informatique »¹ dans sa dernière version. Ces règles sont déclinées par ce qui suit.

L'annexe n°1 de l'IGI 1300 prévoit que les systèmes d'information aptes à traiter des informations DR doivent faire l'objet d'une homologation de sécurité (§ 5). En conséquence, les Systèmes d'Information (SI) utilisés par le soumissionnaire et ses éventuels cotraitants et sous-traitants pour traiter et élaborer les documents DR dans le cadre de la consultation doivent être :

- des SI homologués par l'Autorité Qualifiée de l'entreprise, aptes à traiter des informations classifiées ;
- ou des SI homologués par l'Autorité Qualifiée de l'entreprise conformément aux dispositions de l'II 901, aptes à traiter des informations DR ;
- ou, dans l'attente d'une homologation, des SI constitués d'un ordinateur ou d'un réseau qui obéissent aux règles suivantes :
 - o Le système est dédié aux applications bureautique propres à l'entreprise ;
 - o Le système ne possède aucune connexion avec l'Internet² ;
 - o Le système est conforme aux règles de configuration et utilisation définies à l'article 3.

¹ Document disponible sur le site de l'ANSSI (<http://www.ssi.gouv.fr>)

² Filare, WIFI, GSM, etc.

ARTICLE 3 - REGLES DE CONFIGURATION ET D'UTILISATION

3.1 PROTECTION DU SYSTEME INFORMATIQUE

Le système informatique (postes de travail informatiques, applications bureautiques) est propre à l'entreprise et ne peut être externalisé ou hébergé par un tiers (pas de solution bureautique en nuage). Conformément à l'II 901 – Annexe 2, à défaut de passerelle d'interconnexion homologuée, le réseau utilisé doit être un réseau de classe 2, isolé c'est-à-dire non connecté même indirectement à internet. Les transferts vers ce type de réseau doivent être réalisés au travers de diode agréée par l'ANSSI ou par le biais de supports amovibles contenant les informations chiffrées transmises par le CEA.

Le système informatique est protégé par un antivirus efficace mis à jour régulièrement, au minimum de manière hebdomadaire et l'accès aux informations sensibles est restreint aux seules personnes ayant à les consulter et les traiter, via un compte nominatif et un mot de passe robuste.

3.2 SAUVEGARDES

Le soumissionnaire souhaitant sauvegarder des informations portant la mention de protection DR, s'engage à mettre en œuvre sous sa responsabilité, une sauvegarde de ces informations dans des conditions telles que l'on puisse localiser et identifier le ou les supports de sauvegarde. Le support de sauvegarde pourra être :

- des CD ROM ou DVD ROM : Ceux-ci devront alors porter la mention « Diffusion Restreinte » et être stockés dans une armoire fermée à clefs.
- une ou plusieurs machines du réseau spécifique.

A l'issue de la consultation, les supports de sauvegarde devront être remis au CEA ou faire l'objet d'une destruction conformément aux dispositions de l'article 5 du présent engagement.

3.3 SUPPORTS AMOVIBLES

Si le soumissionnaire souhaite utiliser des supports informatiques amovibles dans le cadre de la consultation, ces derniers devront être des clefs USB, des CD-ROM ou des disques amovibles. Le soumissionnaire s'engage à ce que ces supports répondent aux conditions mentionnées ci-dessous :

- les supports sont neufs ou ont été reformatés par un outil approuvé par l'ANSSI,
- ils sont parfaitement identifiés,
- ils sont dédiés à l'affaire en cours,
- les clefs USB ne sont pas utilisées pour faire du stockage ou de l'archivage de données (précaution technique).

Tous les fichiers relatifs à la consultation contenant des informations DR, déposés sur ces supports, doivent être chiffrés suivant les dispositions de l'article 4.2.

Nota : Les fichiers n'ayant pas de caractère sensible tels que des documents administratifs, plaquettes d'entreprise, etc., qui sont de Diffusion Ordinaire ou publics, peuvent être non chiffrés.

A l'issue de la consultation, les fichiers et supports amovibles devront être remis au CEA ou faire l'objet d'une destruction ou d'un effacement sécurisé conformément aux dispositions de l'article 5 infra.

ARTICLE 4 - COMMUNICATIONS PAR VOIE ELECTRONIQUE

4.1 PRINCIPES GENERAUX

Le soumissionnaire s'engage à appliquer les règles suivantes pour toute communication par voie électronique réalisée dans le cadre de la consultation (et notamment toute communication entre les membres de son personnel, avec ses cotraitants et sous-traitants ou avec le CEA).

1. Aucun message de niveau DR (corps du message et pièce jointe) n'est transmis en clair sur Internet.
2. Tout document de niveau DR y compris lorsqu'il est échangé au moyen de la plateforme de dématérialisation des achats utilisée par le CEA doit être transmis dans des conteneurs chiffrés suivant les dispositions des articles 4.2 et 4.3.

4.2 MANIPULATION DES CONTENEURS CHIFFRES

Les soumissionnaires disposant préalablement du logiciel de chiffrement ACID Cryptofiler peuvent échanger avec le CEA par ce moyen. Pour ce faire, les clés publiques ACID des correspondants peuvent être échangées sur l'Internet.

A défaut, le logiciel de chiffrement ZoneCentral ou Zed sont utilisés. Pour ce faire, dans le cadre d'un dossier de consultation des entreprises, un conteneur Zed vide est mis à disposition des soumissionnaires sur la plateforme de dématérialisation des achats utilisée par le CEA. Le mot de passe d'accès est transmis aux personnes concernées par une voie spécifique (courrier, téléphone). Le mot de passe, qu'il est conseillé de noter dans un document protégé de niveau DR, n'est écrit sur aucun système informatique ni téléphone mobile. Les conteneurs Zed doivent être utilisés uniquement à l'aide du logiciel ZoneCentral ou la version qualifiée gratuite du logiciel Zed disponible sur le site de l'éditeur Prim'x (<http://zedle.primx.eu/>).

Les conteneurs chiffrés, Zed ou ACID, sont transférés sur le SI sécurisé du soumissionnaire tel que défini à l'article 2 préalablement au traitement des documents qu'ils contiennent. Symétriquement, les documents à expédier sont mis en conteneur sur le SI sécurisé, avant expédition en pièce jointe de messagerie ou dépôt sur la plateforme d'échange avec le CEA.

Un document d'initiation au fonctionnement de Zed est disponible auprès du CEA.

4.3 POLITIQUE DES MOTS DE PASSE

Les règles minimales pour la composition des mots de passe sont décrites ci-après. Elles sont appliquées pour les grands réseaux de la DAM et ainsi qu'à ceux appartenant aux entreprises.

- Longueur minimale : 12 caractères ;
- Composition : nombre de jeux de caractères différents : 3 ;
- Historique (nombre des derniers mots de passe non réutilisables) : 6 ;
- Nombre maximal de tentatives avant blocage du compte : 3 ;
- Durée de vie maximale (durée au-delà de laquelle le compte est verrouillé, avec changement obligatoire lors du déverrouillage) : 1 an ;
- Durée de vie minimale (durée pendant laquelle un second changement est impossible) : 5 jours ;
- Incitation à changer (préannonce d'expiration) : 15 jours.

EXIGENCES DE COMPOSITION

- Ne pas contenir 5 caractères consécutifs du nom, prénom, numéro de badge du salarié ou dernier mot de passe;
- Ne pas contenir un mot issu d'un dictionnaire (français, anglais) ni, autant que possible, des combinaisons triviales (1234, azerty, etc.) ;
- Ne pas contenir plus de 2 fois consécutives le même symbole

ARTICLE 5 - FIN DE PROCEDURE - RESTITUTION

A la fin de la consultation, si votre entreprise n'est pas retenue pour ce marché, vous devrez retourner ou détruire l'intégralité des informations ou supports sensibles portant la mention « diffusion restreinte » mis à votre disposition dans le cadre de la présente procédure/consultation. Tous les fichiers DR traités, ainsi que les dossiers de travail et les sauvegardes de niveau DR devront être supprimés selon une procédure d'effacement sécurisé³. Les supports amovibles seront détruits ou remis au CEA. Une attestation sur l'honneur de destruction ou d'effacement des informations DR et supports amovibles sera alors adressée au CEA.

Nous vous rappelons que la conservation, la copie, la diffusion de ces informations ou supports sensibles, sans autorisation écrite et préalable du CEA, est susceptible d'engager votre responsabilité.

En cas d'attribution du marché, le Titulaire s'engage à respecter les dispositions de restitution figurant dans les documents applicables au marché.

ARTICLE 6 - AUDIT ET CONTROLE

Au titre de la Protection du Patrimoine Scientifique et Technique (PPST) pour le compte du Haut Fonctionnaire de Défense et de Sécurité (HFDS) du Ministère de tutelle du CEA, le CEA pourra être amené à auditer les conditions de protection des informations de Diffusion Restreinte du CEA.

ARTICLE 7 - ENGAGEMENT DU SOUMISSIONNAIRE

La société (1)....., immatriculée au Registre du Commerce et des Sociétés sous le numéro (2)....., représentée par (3)....., s'engage par les présentes à respecter l'ensemble des règles fixées dans le présent document.

(1) *Indiquer la raison sociale de l'entreprise*

(2) *Préciser au format : RCS + ville + « B » + numéro*

(3) *Mentionner le nom et la fonction du représentant*

Date :

Signature :

Cachet de l'entreprise :

³ La suppression effective des fichiers exige de réécrire des données sur l'espace mémoire ou disque qu'ils occupaient, par « surcharge » de cet espace.