

Direction de la mémoire, de la culture
et des archives

Service historique de la Défense
Secrétariat général
Bureau finances et achats

Objet de la consultation : Décontamination des magasins d'archives et des archives contenant des informations et supports classifiés ainsi que le reconditionnement de ces archives conservées sur le site de Brest du Service historique de la Défense

PHASE CANDIDATURE

ANNEXE - PROTECTION DE L'INFORMATION DE DIFFUSION RESTREINTE- REGLES DE SÉCURITÉ INFORMATIQUE

La présente annexe doit signée par le candidat et chaque sous-traitant du candidat 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 puis retournée au « contact contractuel » mentionné au début du présent règlement avant toute communication de documents portant la mention « diffusion restreinte » (DR).

Engagement du soumissionnaire en matière de protection de l'information de diffusion restreinte - déclinaison en règles de sécurité informatique

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
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
SI	Système d'Information

SSI	Sécurité des Systèmes d'Information
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 procédures de passation de marché public du SHD qui échangent des informations portant la mention « diffusion restreinte » (DR).

Ce document doit être signé par un représentant du candidat ayant tout pouvoir à cet effet.

Un exemplaire de ce document doit être rempli et retourné pour chaque sous-traitant du soumissionnaire 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 le guide ANSSI « Maitriser la SSI pour les systèmes industriels » V1.0 de janvier 2014 et les prescriptions spécifiques au marché.

ARTICLE 2 - EXIGENCES DE SECURITE INFORMATIQUE

Les soumissionnaires aux procédures de passation de marché public du Service historique de la Défense (SHD) s'engagent à traiter les 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 09 août 2021 sur la protection du secret de la défense nationale, l'instruction interministérielle relative à la protection des systèmes d'informations sensibles n° 901/SGDSN/ANSSI (II 901) et, en conséquence, le guide ANSSI « Hygiène Informatique »4 dans sa dernière version. Ces règles sont déclinées infra.

L'annexe 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. En conséquence, les Systèmes d'Information (SI) utilisés par les soumissionnaires pour traiter et élaborer les documents DR doivent être des SI homologués par l'Autorité d'Homologation (désignée par l'Autorité Qualifiée en Sécurité des Systèmes d'information de l'organisme dont dépend l'utilisateur) conformément aux dispositions de l'II 901, aptes à traiter des informations DR.

Dans le contexte de cette homologation, les SI doivent être conformes aux règles de configuration et d'utilisation définies à l'article 3.

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'organisme 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 peuvent

être réalisés au travers de diode agréée par l'ANSSI ou par le biais de supports amovibles contenant les informations chiffrées transmises par le SHD.

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

Tout 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 chaque consultation, les supports de sauvegarde devront être remis au SHD ou faire l'objet d'une destruction conformément aux dispositions de l'article 5.

3.3 SUPPORTS AMOVIBLES

Tout soumissionnaire souhaitant utiliser des supports informatiques amovibles, s'engage à ce que ces derniers soient des clefs USB, des CD-ROM ou des disques amovibles. Il s'engage également 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.

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

ARTICLE 4 - COMMUNICATIONS PAR VOIE ELECTRONIQUE

4.1 PRINCIPES GENERAUX

Chaque soumissionnaire s'engage à appliquer les règles suivantes pour toute communication par voie électronique :

- Aucun message de niveau DR (corps du message et pièce jointe) n'est transmis ou diffusé en clair sur Internet.
- Tout document portant la mention de protection DR échangé doit être transmis dans des conteneurs chiffrés suivant les dispositions de l'article 4.2.

4.2 MANIPULATION DES CONTENEURS CHIFFRES

Les logiciels de chiffrement utilisés au SHD sont : ZoneCentral ou Zed. Le mot de passe d'accès à un conteneur Zed est transmis aux personnes concernées par une voie spécifique (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/>).

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

ARTICLE 5 - FIN DE PROCEDURE - RESTITUTION

A la fin de chaque consultation, les entreprises non retenues devront retourner ou détruire l'intégralité des informations ou supports sensibles portant la mention « diffusion restreinte » mis à leur disposition dans le cadre de la présente procédure. 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 sécurisé⁵. Les supports amovibles seront détruits ou remis au SHD.

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

ARTICLE 6 - ENGAGEMENT DE L'UTILISATEUR

Je soussigné M. / Mme, m'engage par les présentes à respecter l'ensemble des règles fixées dans le présent document.

Date :

Signature :