

ANNEXE N° X AU CAHIER DES CLAUSES TECHNIQUES PARTICULIERES

DE L'ACCORD-CADRE SAJ-DSSE N° AA-NN

DOCUMENT DE REFERENCE DES CLAUSES DE SECURITE DU SYSTEME D'INFORMATIONS

Table des matières

1. Introduction.....	2
2. Clause de confidentialité type en cas de sous-traitance.....	2
3. Clauses de sécurité types	2
3.1 Gestion de la sécurité.....	3
3.2 Protection antivirale.....	3
3.3 Mises à jour, correctifs de sécurité	3
3.4 Sauvegardes et restauration	4
3.5 Continuité d'activité.....	4
3.6 Authentification.....	5
3.7 Confidentialité et intégrité des flux.....	5
3.8 Contrôle et filtrage des flux.....	6
3.9 Imputabilité, traçabilité.....	6
3.10 Marquage des supports de données et équipements sensibles.....	7
3.11 Personnels en charge des prestations.....	7
3.12 Qualifications et expérience, formations et sensibilisation dans le domaine de la SSI des personnels en charge des prestations.....	7
3.13 Exigences de sécurité concernant les personnels extérieurs (maintenance, entretien...)	7
3.14 Continuité des services essentiels : énergie, climatisation et télécommunications.....	8
3.15 Protection contre les incendies, la foudre et les dégâts des eaux.....	8
3.16 Surveillance et contrôle des accès aux locaux de l'hébergeur, en particulier au local d'hébergement du système d'information	8
3.17 Intervention des sociétés de maintenance ou de support de solutions informatiques (matérielles ou logicielles).....	9
3.18 Audits de sécurité.....	9
3.19 Convention de service	10

1. Introduction

Ce document est une annexe au Cahier des Clauses Techniques Particulières. Il contient les exigences de sécurité à remplir pour le prestataire. Certaines de ses exigences font directement référence au CCTP.

2. Clause de confidentialité type en cas de sous-traitance

Les supports informatiques et documents fournis par l'Amue à la société [identité du prestataire] restent la propriété de l'Amue.

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 [identité du prestataire] 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 [identité du prestataire] 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 [identité du prestataire] 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 [identité du prestataire] ne pourra sous-traiter l'exécution des prestations à une autre société, ni procéder à une cession de marché sans l'accord préalable de l'Amue.

L'Amue se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect des obligations précitées par la société [identité du prestataire].

3. Clauses de sécurité types

Avertissement : les exigences de sécurité qui suivent doivent être sélectionnées avec prudence, d'une part en fonction des spécificités du système d'information, d'autre part en tenant compte de la nature des prestations externalisées.

3.1 Gestion de la sécurité

Le candidat précisera les moyens mis en œuvre dans le cadre du processus d'amélioration continu de la sécurité de ses infrastructures d'hébergement.

Cette description peut être avantageusement présentée selon les 4 étapes de la méthode de gestion de la qualité PDCA (*Plan-Do-Check-Act*) :

- phase de préparation ;
- phase de réalisation ;
- phase de vérification : préciser la fréquence ainsi que le périmètre technique et organisationnel des audits réalisés en interne par les équipes du prestataire ou par une société tierce ;
- phase d'ajustement (mesures correctives suite aux insuffisances constatées lors de la vérification).

3.2 Protection antivirale

Une politique antivirale stricte devra être mise en place au niveau des serveurs dont le titulaire a la charge. La mise à jour des signatures devra être automatique et d'une fréquence élevée (30 minutes).

La politique antivirale appliquée sur le système d'information du titulaire devra être précisée (postes de travail des exploitants notamment).

Le candidat fournira dans sa réponse une description des solutions anti-virus sur lesquelles se base son service de messagerie (logiciel, version) et décrira les modalités et la fréquence de mise à jour du service.

Un contrôle de non contamination des serveurs Web de production devra être effectué périodiquement. Le candidat précisera les modalités de mise en œuvre de ce contrôle.

3.3 Mises à jour, correctifs de sécurité

Le titulaire applique les correctifs recommandés par les fournisseurs de solutions matérielles ou logicielles (logiciels système ou applicatifs, logiciels embarqués) sur tous les matériels dont il a la charge.

En cas d'alerte grave (attaque virale, faille critique) annoncée par le CERT-FR (French Computer Emergency Response Team), le correctif doit être appliqué dans un délai de 24 heures sur les infrastructures hébergeant le système du donneur d'ordres (serveurs, pare-feu, routeurs ouverts vers l'extérieur).

Lorsqu'aucun correctif n'est pas disponible, le titulaire doit suivre les recommandations de l'éditeur ou du CERT-FR dans le cadre d'un contournement provisoire. Si le contournement nécessite la désactivation d'une fonctionnalité indispensable au système, le titulaire s'engage à proposer des mesures permettant d'éviter l'exploitation de la vulnérabilité.

Le traitement des alertes mineures pourra intervenir durant les périodes de maintenance hebdomadaires ou mensuelles.

Les passages de correctifs doivent être précédés d'une sauvegarde spécifique du système et des données qu'il contient, ainsi que de tests sur un environnement de pré production.

Le titulaire devra mettre à jour le dossier de définition avec la liste des correctifs de sécurité appliqués sur les serveurs et communiquer au donneur d'ordres la version actualisée du document.

La validation du bon fonctionnement du système se fera conjointement avec les équipes techniques du titulaire et le chef de projet responsable de l'application hébergée.

En cas d'alerte donnée par les équipes d'experts du titulaire, par l'administration ou le CERT-FR, le maître d'ouvrage sera notifié par téléphone et courrier électronique avant toutes opérations. La décision de l'action ne pourra être prise que par des personnels de la maîtrise d'ouvrage désignés par écrit. En particulier, le responsable sécurité de la maîtrise d'ouvrage sera le correspondant privilégié pour le suivi des opérations.

Le titulaire s'engage à fournir une adresse mail, un numéro de téléphone et les périodes correspondantes d'opération (H24, heures ouvrables, ...) permettant au maître d'ouvrage de suivre le traitement d'une alerte.

3.4 Sauvegardes et restauration

Le titulaire doit prendre toutes les mesures qui s'imposent en termes de sauvegarde et de restauration pour se conformer au niveau de service exigé.

Les opérations de sauvegardes donnent lieu à un compte-rendu par messagerie avec indicateur de réussite ou d'échec.

La fiabilité des sauvegardes sera mise à l'épreuve par des tests de restauration mensuels, dont les rapports seront communiqués dans le mois suivant les tests.

Un double exemplaire des sauvegardes doit être conservé dans des locaux physiquement séparés du centre informatique du prestataire hébergeant l'application du donneur d'ordres.

Le titulaire doit prendre des mesures permettant de garantir la confidentialité des données relatives aux sauvegardes :

- confidentialité des flux lors des opérations de sauvegardes ;
- stockage sécurisé des sauvegardes.

En cas de sauvegarde externalisée, les sauvegardes doivent être chiffrées avant leur transfert et la clé de chiffrement connue seulement du titulaire et du donneur d'ordres.

Dans le cadre de plans de sécurité gouvernementaux, le donneur d'ordres pourra imposer une augmentation de la fréquence des sauvegardes.

3.5 Continuité d'activité

Le titulaire doit prendre toutes les mesures nécessaires pour assurer la disponibilité du système d'information, conformément aux exigences définies dans la clause relative au niveau de service exigé.

Le candidat indiquera les mesures techniques, organisationnelles, procédurales qu'il s'engage à prendre pour assurer la continuité d'activité du système, ou en cas de sinistre la reprise d'activité conformément aux exigences définies dans la clause sur la convention de service.

Les procédures de sauvegarde et de secours seront auditées conformément aux modalités identifiées dans la clause relative aux audits de sécurité.

3.6 Authentification

Pour chaque interface d'accès au système, (Interface Homme-Machine, interface entre applications) le titulaire doit fournir une documentation précisant :

- les mécanismes d'authentification mis en œuvre (protocoles, algorithmes de hachage et de chiffrement utilisés) ;
- la liste exhaustive des comptes d'accès existants ainsi que des rôles et privilèges qui y sont associés.

Les moyens d'authentification associés aux interfaces doivent être interopérables tant au niveau des applications clientes (par exemple navigateurs web) que des systèmes d'exploitation.

Les interfaces d'accès aux fonctionnalités bas niveau (exemple : configuration du BIOS) doivent impérativement authentifier un utilisateur (mise en place d'un mot de passe pour l'utilitaire de configuration du BIOS).

Les identifiants des comptes d'accès sont nominatifs. L'utilisation d'un même compte par plusieurs personnes n'est pas autorisée sauf si une contrainte le justifiant est acceptée par le donneur d'ordres. Dans ce cas, le candidat présentera les mesures techniques et/ou organisationnelles pour garantir l'imputabilité. L'utilisation de mots de passe constructeur ou par défaut est interdite.

L'utilisation de protocoles dont l'authentification est en clair est interdite

Les mots de passe doivent satisfaire aux contraintes de complexité suivantes :

- Avoir une longueur minimale de 14 caractères (sauf limitation technique) ;
- Comporter au minimum une majuscule, un chiffre et un caractère spécial ;
- Ne pas être vulnérables aux attaques par dictionnaire.

L'utilisation de certificats clients et serveurs pour l'authentification est une alternative préférable aux mots de passe à condition que la clef privée soit protégée dans un matériel adéquat.

Les mots de passe et secret doivent être stockés dans un conteneur sécurisé (type vault ou coffre-fort).

3.7 Confidentialité et intégrité des flux

Tous les flux d'administration doivent être chiffrés par des procédés fiables (SSH, SSL, IP sec, etc...), garantissant la confidentialité et l'intégrité des données.

De façon générale, tous les flux contenant des informations sensibles et circulant sur un réseau public doivent être chiffrés par des procédés apportant ces mêmes garanties.

Le choix et le dimensionnement des algorithmes cryptographiques doivent être effectués conformément aux règles et recommandations du RGS en la matière.

Le candidat indiquera l'ensemble des mécanismes et mesures mis en œuvre pour garantir la confidentialité et l'intégrité des flux d'administration.

3.8 Contrôle et filtrage des flux

Au titre de la défense en profondeur, trois zones seront mises en place, chacune étant protégée par un dispositif de filtrage :

- Une zone publique regroupant les machines qui hébergent des services ayant vocation à communiquer avec l'extérieur (Reverse Proxy, Serveur Web, FTP, Serveur de mail, DNS ,etc.);
- une zone privée regroupant les machines n'ayant pas vocation à communiquer avec l'extérieur;
- un réseau dédié à l'administration des machines et des équipements à partir de postes de travail situés chez l'hébergeur.

Le trafic réseau en provenance et à destination du système doit faire l'objet d'un contrôle permanent afin de n'autoriser que les flux légitimes. Une matrice de flux (inventaire des flux légitimes) sera fournie par le prestataire.

La politique de filtrage est définie à partir de la matrice des flux. Les dispositifs de filtrage sont bloquants par défaut, tout ce qui n'est pas explicitement autorisé étant interdit.

Le service global doit être protégé contre les attaques classiques sur IP et les protocoles associés (filtrage sanitaire) notamment :

- attaque en déni de service (*TCP SYN Flood, Ping Flooding, SMURF, Ping of Death, large packet attacks*, etc.) ;
- IP options (*source routing*, etc.).

Le candidat décrira dans sa réponse les différents mécanismes de protection prévus au niveau des équipements pour contrer les attaques classiques sur IP et les protocoles associés.

Les interfaces d'administration des machines ou des équipements du système ne doivent pas être accessibles depuis l'extérieur. Les services correspondants seront donc configurés pour ne pas accepter de connexions sur les interfaces publiques.

Seuls les services utiles au bon fonctionnement de l'application doivent être activés. Les autres services doivent être désactivés et si possible désinstallés.

3.9 Imputabilité, traçabilité

Les informations suivantes devront être enregistrées :

- entrée en session d'un utilisateur : date, heure, identifiant de l'utilisateur et du terminal ; réussite ou échec de la tentative ;
- actions qui tentent d'exercer des droits d'accès à un objet soumis à l'administration des droits : date, heure, identité de l'utilisateur, nom de l'objet, type de la tentative d'accès, réussite ou échec de la tentative ;
- création/suppression d'un objet soumis à l'administration des droits : date, heure, identifiant de l'utilisateur, nom de l'objet, type de l'action ;
- actions d'utilisateurs autorisés affectant la sécurité de la cible : date, heure, identité de l'utilisateur, type de l'action, nom de l'objet sur lequel porte l'action.

3.10 Marquage des supports de données et équipements sensibles

Préciser les mesures mises en œuvre pour assurer le recensement, la classification et le suivi des supports de données et équipements sensibles (boîtiers de chiffrement, pare-feu, etc.)

Le marquage des supports de stockage de données est obligatoire (disque dur, bandes de sauvegardes, etc.).

3.11 Personnels en charge des prestations

Le titulaire s'engage à fournir une liste, régulièrement mise à jour, des personnels autorisés à intervenir sur le système d'information du maître d'ouvrage ainsi que leur niveau d'habilitation (types d'accès et ressources concernées du client).

Le candidat précisera les moyens mis en œuvre, dans le cadre de son processus de recrutement du personnel, pour vérifier les éventuelles condamnations, le cursus et l'expérience professionnelle des futurs employés.

Si le candidat ou des employés de son entreprise possèdent une habilitation au niveau Confidentiel-Défense, il pourra en faire mention.

Le candidat précisera dans son offre si d'autres clients peuvent accéder aux mêmes locaux que ceux utilisés par le maître d'ouvrage et dans quelle mesure il sera possible de limiter ces accès à la demande de ce dernier.

Dans le cadre de plans de sécurité gouvernementaux, le donneur d'ordres pourra imposer un renforcement des contrôles d'accès physiques et logiques à ces équipements.

3.12 Qualifications et expérience, formations et sensibilisation dans le domaine de la SSI des personnels en charge des prestations

Le candidat indiquera dans sa réponse :

- les qualifications, diplômes ainsi que le niveau d'expérience des personnels retenus pour la réalisation des prestations d'infogérance ;
- la fréquence et le contenu des actions de formation et de sensibilisation des personnels aux enjeux de sécurité.

3.13 Exigences de sécurité concernant les personnels extérieurs (maintenance, entretien...)

Le candidat précisera les moyens de contrôle mis en œuvre pour s'assurer du respect des exigences de sécurité du donneur d'ordres par ses sous-traitants éventuels, ainsi que des consultants ou techniciens amenés à intervenir dans le cadre du support et de la maintenance sur le système du client. Cette exigence peut être étendue à tous les types de soutiens (ménage, chauffage, climatisation, etc) si la sensibilité du système le justifie.

3.14 Continuité des services essentiels : énergie, climatisation et télécommunications

Une solution de secours doit être mise en œuvre en cas de dysfonctionnement de l'alimentation électrique, de la climatisation ou des moyens de communication.

Le candidat décrira les moyens mis en œuvre afin d'assurer la continuité des services essentiels (énergie, climatisation, télécommunications) sur le site d'exploitation du système :

- situation et caractéristiques générales du site d'exploitation ;
- protection et redondance électriques (groupes électrogènes, onduleurs,
- protection contre les surtensions, etc.) ;
- contrats de service avec les fournisseurs d'accès, caractéristiques des liaisons de secours ;
- systèmes de climatisation ;
- moyens de supervision et remontées d'alarme ;
- les équipements utilisés par le système du donneur d'ordres, en particulier les composants redondants seront décrits (alimentations, disques, cartes contrôleurs, serveurs, équipements réseau, liens réseau) ;
- le candidat précisera les éventuels agréments gouvernementaux ou certificats de conformités qu'il détient.

3.15 Protection contre les incendies, la foudre et les dégâts des eaux

Le candidat décrira les moyens mis en œuvre en ce qui concerne :

- la prévention, la détection et le traitement des incendies ;
- la protection contre les dégâts des eaux ;
- la protection contre la foudre et les surtensions.

Il sera notamment indiqué dans la réponse si les bâtiments du site d'exploitation se situent ou non en zone inondable.

3.16 Surveillance et contrôle des accès aux locaux de l'hébergeur, en particulier au local d'hébergement du système d'information

Le site d'hébergement doit être surveillé 24h/24 et 7j/7.

Le titulaire doit mettre en œuvre un dispositif permettant de réserver l'accès aux locaux hébergeant l'ensemble des machines et postes de travail utilisés aux seules personnes autorisées par le client : filtrage des accès au bâtiment ou aux étages, et filtrage des accès aux salles machines. Il définira les conditions d'accès du client au service (horaires d'ouverture, cas d'indisponibilité ponctuelle, etc.).

Le candidat doit détailler tous les moyens mis en œuvre afin d'assurer la sécurité des locaux d'hébergement, notamment :

- moyens de surveillance, dispositifs anti-intrusion ;
- contrôle et enregistrement des accès (gardiennage, sas, moyen d'identification, etc.) ;
- protection physique des équipements (verrouillage des baies, etc.).

3.17 Intervention des sociétés de maintenance ou de support de solutions informatiques (matérielles ou logicielles)

Les intervenants des sociétés assurant la maintenance ou le support technique de solutions doivent être accompagnés par une personne habilitée à intervenir sur le système pendant toute la durée de leur intervention. Si un intervenant a besoin de se connecter au système, il doit utiliser un compte spécifique permettant de garantir l'imputabilité de ses actions.

Le candidat présentera les mesures techniques et organisationnelles pour empêcher les extractions massives d'information (par exemple : extraction d'une copie de la base de données à partir d'un poste dédié à l'administration).

Les supports de stockage de données (disques durs, bandes de sauvegardes, etc.) restent la propriété du client. Ils ne peuvent être mis au rebut ou emportés par une société de maintenance, ou encore réutilisés à d'autres fins que celles prévues initialement sans l'autorisation expresse du donneur d'ordres.

Ils doivent être conservés en lieu sûr par le titulaire, en attendant de procéder à leur effacement ou à leur destruction avec des moyens adaptés visant à s'assurer qu'aucune donnée ne puisse être récupérée. L'effacement ou la destruction ont lieu en présence d'un représentant du donneur d'ordres.

3.18 Audits de sécurité

Le client doit pouvoir, à tout moment, contrôler que les exigences de sécurité sont satisfaites par les dispositions prises par le prestataire.

Le périmètre et la périodicité des audits de sécurité doivent être précisément définis.

Les audits pourront être réalisés par le client, ou délégués à un tiers. Le contrôle s'effectuera selon des modalités contractuelles définies (visite des locaux du prestataire avec interviews individuelles des membres des équipes du prestataire, accès aux machines mises à la disposition du prestataire).

Cette visite sera notifiée au prestataire selon un délai prévu par le contrat. Un délai de 15 jours est recommandé car il permet à l'hébergeur de s'organiser (rassembler la documentation, s'assurer de la disponibilité des personnes concernées).

Le cas d'une intervention urgente du fait, par exemple, de la survenance d'un incident de sécurité à traiter doit être prévu.

La pratique de tests intrusifs doit être encadrée par une charte commune signée entre le prestataire, l'exécutant de l'audit et le client.

Le client doit se réserver le droit de requérir l'expertise d'un organisme ou d'une société tierce présentant des compétences en matière de sécurité.

3.19 Convention de service

Cette clause est la formalisation d'un accord entre le prestataire et le client relatif au niveau de service attendu (*Service Level Agreement*). Ainsi, il pourra être demandé au prestataire des engagements concernant :

- le taux de disponibilité du système (en heures ouvrées / non ouvrées) ;
- la durée et l'occurrence maximale d'indisponibilité mensuelle, trimestrielle ou annuelle d'un composant ou du système ;
- le temps de réponse d'une application ou de certaines requêtes, la durée maximale de certains traitements ;
- le temps garanti d'intervention sur site (GTI) ;
- le temps garanti de remise en état d'un composant matériel ou logiciel défectueux (GTR), ou d'une chaîne de liaison ;
- le temps moyen entre deux pannes (MTBF) ;
- le taux de panne mensuel, trimestriel ou annuel d'un composant ou du système (taux de fiabilité).

Ces engagements pourront être définis pendant une phase probatoire, et réajustés à l'issue de celle-ci. Ils pourront également être redéfinis en cas de modification du périmètre de l'opération.

Les niveaux d'engagement, de même que les pénalités en cas de non-respect de ces derniers, seront négociés selon les spécificités de chaque projet.