

ANNEXE AU CCTP

CLAUSES DE SÉCURITÉ DES SYSTEMES D'INFORMATION

1. Etat de l'art

Conformément à l'article 10.8 du CCAP, le titulaire conçoit, met en œuvre et exploite les systèmes d'informations sous sa responsabilité conformément à l'état de l'art en matière de sécurité des systèmes d'information. Il doit se reporter systématiquement aux guides de recommandations de l'ANSSI pour être à jour de l'état de l'art en la matière. Toutefois, il doit respecter les exigences suivantes pour les services Web et de messagerie :

- Interfaces web :
 - les développements ne doivent pas générer d'adhérence avec des modules spécifiques (Flash, Silverlight, JRE, etc.) ou une technologie en particulier ;
 - les mécanismes cryptographiques TLS (https) doivent être systématiquement activés pour identifier et authentifier la source et protéger les communications ; l'utilisation de la technologie HSTS est fortement recommandée ;
 - les mécanismes de protection des cookies de session (HttpOnly, Secure, SameSite) sont mis en œuvre pour se protéger des vols ou exploitation de sessions déjà ouvertes ;
 - une politique de sécurité des contenus (CSP, SRI) et des navigateurs (emploi d'entêtes de sécurité (X-Content-Type-Options, X-Frame-Options, X-XSS-Protection, Referrer-Policy) est élaborée pour se protéger contre les injections de contenus actifs malicieux ;
 - les obligations légales sont renseignées sur les sites Internet et un point de contact est publié via le fichier /.well-known/security.txt pour permettre des signalements directement auprès des points de contact identifiés.
- Services de courriels :
 - les mécanismes de chiffrement TLS sont mis en œuvre pour l'authentification, la lecture et la distribution des messages (STARTTLS, SMTPS, IMAPS, etc.) ;
 - la mise en œuvre des mécanismes permettant de garantir l'authenticité des émetteurs est systématiquement envisagée (contrôle des noms de domaines associés aux serveurs (SPF), signature numérique (DKIM), politique de sécurité liant le tout (DMARC)).

2. Politique, organisation et gouvernance de la sécurité

Politique de sécurité du titulaire :

Le titulaire applique et fait appliquer à ses sous-traitants le cas échéant la politique de sécurité du présent marché. Cette politique de sécurité traite notamment des thèmes suivants :

- Organisation de la Sécurité des SI ;
- Application de la Politique de Sécurité des SI ;
- Évaluation de la sensibilité et protection des documents ;
- Gestion des ressources humaines ;
- Sécurité physique des locaux et des salles informatiques ;
- Architecture et exploitation des SI : réseaux, systèmes ;
- Sécurité des postes de travail ;
- Sécurité des supports numériques ;
- Gestion des autorisations et contrôle d'accès logique aux ressources ;

- Développement et maintenance des systèmes ;
- Gestion des incidents et des alertes ;
- Gestion de la continuité d'activité des SI ;
- Conformité et démarche de contrôle interne ;
- Localisation des données.

Organisation de la sécurité adéquate :

Le titulaire définit une organisation de la sécurité afin de respecter l'ensemble des contraintes émises par l'acheteur.

Existence d'un correspondant de sécurité :

Le titulaire désigne parmi son personnel un correspondant sécurité pour toute la durée de la prestation.

Ce correspondant est notamment :

- L'interlocuteur privilégié de l'acheteur pour toutes les questions relatives à la sécurité de la prestation, notamment dans le cadre d'investigations initiées par l'acheteur ou le titulaire suite à des incidents de sécurité opérationnels ;
Ce correspondant est joignable aux horaires suivants 9h-18h les jours ouvrés. Tout remplacement de ce correspondant doit être notifié à l'acheteur conformément aux dispositions prévues au CCAP. De plus, une suppléance de ce correspondant de sécurité doit être assurée pour pallier son indisponibilité.
- Mise en œuvre d'une gestion de risques et son suivi : le titulaire met en place une gestion des risques et assure un suivi permanent de son niveau de maîtrise de risques ainsi que du respect des politiques et règles de sécurité applicables sur le périmètre des prestations, y compris auprès de ses propres sous-traitants.
- Gestion de crise sécurité : sur son domaine de responsabilité SI, le titulaire applique le processus formalisé et opérationnel de gestion de crise, apte à assurer le traitement d'événements remettant en cause de façon inacceptable pour l'acheteur le respect des engagements de service et de sécurité SI contractualisés.

Ce plan précise au minimum :

- les principes d'escalade (critères de déclenchement, synoptique d'escalade) ;
- la composition de la cellule de crise : fonctions et responsabilités des membres (acheteur et titulaire). La liste nominative des membres et de leurs suppléants est référencée dans un annuaire ;
- Les moyens dédiés à la gestion de crise (salle(s) de crise, procédures opérationnelles, moyens de communication).

3. Gestion des biens

Séparation des données de l'acheteur et des données d'autres clients :

Le titulaire conserve et traite les données de l'acheteur de manière séparée de ses propres données ou de données d'autres clients du titulaire. Le titulaire doit restreindre l'accès aux données de l'acheteur suivant le principe de restriction au besoin d'en connaître.

L'acheteur doit donner ses performances dans le CCTP : droits d'accès, machines virtuelles séparées, disques séparés, machines physiques séparées...

Protection de la documentation de l'acheteur sur support papier :

Le titulaire assure la protection de la documentation de l'acheteur sur support papier au sein des locaux, en la stockant dans des armoires ou des coffres fermés à clé/code par exemple, et sa destruction à la fin de la prestation.

Modalités d'échanges d'informations :

Le titulaire garantit que les modalités de stockage et d'échanges d'informations par mail permettent d'en assurer la confidentialité et l'intégrité.

Échange de supports :

Le titulaire garantit que les supports échangés ou à connecter sur un SI de l'acheteur n'intègrent aucun code malveillant et ont fait l'objet d'un test d'innocuité positif au moyen d'une attestation à fournir à l'acheteur.

Transmission de fichiers sur un support physique :

Toute transmission de fichiers sur un support physique (DAT, CDROM, etc.), par courrier externe ou par porteur, donne lieu à un accusé de réception.

Il doit respecter les règles de protection des informations et documents existant en vigueur au sein de l'acheteur.

De plus, l'ensemble des opérations de transferts de disques durs, de supports d'archives ou de sauvegarde doit être inscrit dans un registre des opérations précisant :

- l'émetteur et le destinataire ;
- le détail des opérations de transferts et notamment le nombre, la date.

Sur simple demande, ce registre est mis à la disposition de l'acheteur adjudicateur par le titulaire.

Marquage des ressources techniques :

Le titulaire applique des règles de marquage sur les ressources techniques (matériels et logiciels informatiques, supports de stockage) et les supports papier pour faire savoir au personnel autorisé que ces éléments contiennent des informations sensibles ou classifiées.

Supports de stockage hébergeant des données de l'acheteur :

Le titulaire conserve en lieu sûr les supports de stockage de données en fin de vie hébergeant des données de l'acheteur, 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.

Le cas échéant, le titulaire ne met pas au rebut ou ne fait pas emporter par une société de maintenance, ou encore réutilise ces supports de sauvegarde à d'autres fins que celles prévues initialement sans l'autorisation expresse de l'acheteur.

Maintien à jour et mise à disposition des données relatives à la prestation :

Le titulaire maintient à jour et est en mesure de mettre à disposition de l'acheteur toutes les données relatives à la prestation.

Le titulaire fournit systématiquement toute la documentation générée dans le cadre de la prestation à l'acheteur pour archive.

4. Sécurité physique

Changement de localisation géographique des services et des données :

En cas de changement de localisation des données ou services, le titulaire en informe préalablement l'acheteur.

Hébergement de données :

À première demande de l'acheteur, le titulaire identifie tous les titulaires techniques hébergeant ou stockant les données et leurs copies, utilisées ou échangées en cours de marché ainsi que leur localisation.

Contrôle d'accès physique aux bâtiments du titulaire :

Les bâtiments du titulaire hébergeant son personnel dans le cadre de la prestation doivent être équipés d'un dispositif de contrôle d'accès individuel. Les accès physiques aux bâtiments en question doivent être restreints aux stricts besoins opérationnels des différentes populations présentes dans les locaux du titulaire.

Le titulaire dispose d'une procédure de gestion des accès physiques aux bâtiments du titulaire. Celle-ci précise au minimum les modalités de gestion des demandes et de suppressions d'accès.

Le titulaire dispose d'une organisation relative à la gestion et au suivi des autorisations d'accès pour les bâtiments du titulaire.

Contrôle des accès aux ressources techniques du titulaire :

Le titulaire garantit que les accès physiques aux salles informatiques sont strictement restreints aux besoins opérationnels des différentes populations présentes sur les sites utilisés dans le cadre de la prestation. Les accès sont équipés d'un dispositif de contrôle d'accès individuel.

Le titulaire dispose d'une procédure de gestion des accès physiques aux locaux techniques du titulaire. Celle-ci précise au minimum les modalités de gestion des demandes et suppressions d'accès.

Le titulaire dispose d'une organisation relative à la gestion et au suivi des autorisations d'accès pour les locaux hébergeant des ressources de l'acheteur et les équipements de sûreté.

Protection intrusion physique des locaux techniques du titulaire :

Les locaux du titulaire qui hébergent ses ressources techniques (serveurs, équipements informatiques, équipements réseaux / télécoms, etc.) sont équipés de moyens de :

- Protection contre l'intrusion et les effractions ;
- Détection d'intrusion et d'effraction reliés à un système de surveillance centralisé ;
- Réaction en cas d'intrusion ou d'effraction.

Ces équipements sont opérationnels 24h/24h et 7j/7j.

Les moyens de protection sont adaptés aux moyens de détection et de réaction.

En particulier, toutes les portes donnant sur l'extérieur du bâtiment ont une méthode automatique de détection d'ouverture. De plus, toute fenêtre raisonnablement accessible est protégée contre les intrusions.

Accompagnement des visiteurs :

Le titulaire dispose d'une procédure spécifique à l'accueil des personnes étrangères à l'organisme. Il dispose également d'une procédure pour l'accès des véhicules au site.

En particulier, les personnes extérieures nécessitant un accès aux salles hébergeant des ressources informatiques (techniciens, visiteurs, maintenance, etc.) sont accompagnées par une personne habilitée.

Protection des plateaux mutualisés :

En cas de mutualisation de ses plateaux, le titulaire met en place les mesures pour protéger les espaces attribués pour la prestation effectuée pour l'acheteur (accès au poste par badge, blocage session automatique après un certain temps d'inutilisation, câble de sécurité pour le matériel fourni par l'acheteur, etc.).

Étanchéité physique des ressources informatiques :

Les salles hébergeant les ressources informatiques utilisées dans le cadre de la prestation ne partagent pas le même bâtiment avec d'autres fonctions, particulièrement des bureaux n'appartenant pas à l'organisation. Si l'espace doit être mutualisé pour des raisons économiques, alors la salle hébergeant des ressources informatiques utilisées dans le cadre de la Prestation de l'acheteur n'a pas de murs adjacents à d'autres bureaux.

Le titulaire met en place des moyens garantissant une étanchéité physique entre les infrastructures physiques dédiées à l'acheteur de celles des autres clients au sein des salles informatiques :

- La salle hébergeant des matériels de l'acheteur doit si possible lui être dédiée ;
- Dans le cas où la séparation physique des salles n'est pas possible, le titulaire fournit à l'acheteur une solution de « suite privative » au sein de la salle multi-clients, isolée physiquement du reste de la salle par un grillage descendant plus bas que le faux plancher et montant plus haut que le faux plafond.

5. Sécurité du poste de travail

Protection contre le vol des postes de travail :

Le titulaire met en place des mécanismes de protection pour prévenir le vol des postes de travail. Le titulaire met notamment en place des câbles antivol de façon systématique.

Chiffrement du poste de travail :

Une solution de chiffrement, si possible qualifiée, est mise à disposition par le titulaire à ses intervenants afin de chiffrer les données sensibles stockées sur les postes de travail, les serveurs, les espaces de travail, ou les supports amovibles.

6. Traitement des incidents

Remontée d'alerte :

Le service de supervision du titulaire met en place un système de remontée d'alerte à l'acheteur, afin de détecter tout comportement anormal sur un périmètre SI lié à la prestation (ex : montée en charge du réseau), vol ou perte d'informations sensibles appartenant à l'acheteur (documentations techniques en particulier).

Enregistrement et traçabilité et gestion des incidents de sécurité : le titulaire assure l'enregistrement et la traçabilité des incidents de sécurité et dispose d'un processus formalisé et opérationnel de gestion des incidents de sécurité sur son domaine SI.

Traitement des incidents de sécurité :

le titulaire contacte les interlocuteurs sécurité de l'acheteur désignés pour signaler tout incident de sécurité SI susceptible d'affecter les données ou le SI de l'acheteur.

De plus :

- si cet incident a lieu sur le SI de l'acheteur, le titulaire participera à la demande de l'acheteur au traitement de l'incident ;
- si cet incident a lieu sur le SI du titulaire, le titulaire autorisera l'acheteur ou un tiers désigné à participer au traitement de l'incident (si l'acheteur le souhaite).

En outre, des réunions périodiques d'analyse post-incident devront être planifiées avec l'acheteur (traitement des causes profondes).

Base de connaissance :

Le titulaire capitalise les procédures de résolution des problèmes techniques récurrents dans une base de connaissance dédiée qu'il fournit à l'acheteur sur demande.

7. Disponibilité des données et des systèmes d'information

Durant le marché, le titulaire maintient la disponibilité des données (quel que soit leur support), leur conservation et la disponibilité des systèmes d'information dans un délai maximum de 3 jours (à compléter).

En cas de non-respect de ces délais, l'acheteur applique les pénalités visées à l'article XX du CCAP.

L'acheteur précise les performances de disponibilité attendues dans le CCTP.

8. Continuité des services

Remplacement du matériel endommagé ou perdu :

Le titulaire prend toutes les dispositions nécessaires (matériel en spare, contrats de service), en relation avec l'acheteur, pour remplacer rapidement et sur les différents sites de l'acheteur tout matériel sous sa responsabilité endommagé ou perdu (poste de travail, serveur, équipement réseau).

Incident affectant la continuité des services :

En cas d'incident affectant la continuité des services, le titulaire signale l'événement à l'acheteur selon la procédure d'alerte qu'il a définie à l'article Partie : 6 du CCTP (directive de gestion des alertes, incidents et situations de crise).

9. Conformité, audit, inspection, contrôle

Autocontrôles de sécurité :

Le titulaire effectue des autocontrôles de conformité aux exigences du **CCTP** pour garantir le niveau de sécurité au démarrage de la prestation ainsi que son maintien tout au long de la prestation.

Régularisation des écarts ou des non-conformités au niveau d'exigence de sécurité de l'acheteur :

(En cas de constatation d'écarts avec le **CCTP** et, plus généralement,) en cas de non-conformité au niveau d'exigence de sécurité requis par l'acheteur, un plan de remédiation devra être formalisé par le titulaire 15 jours après la constatation des écarts. Le titulaire doit ensuite régulariser ces écarts par l'application du plan de remédiation dans un délai convenu en commun accord entre les deux parties.

La fréquence minimale est définie dans le contrat. Sur la base de ces contrôles effectués, le titulaire doit rendre compte des résultats à l'acheteur à l'occasion de comités de sécurité.

10. Obligations relatives à l'intervention du titulaire dans les locaux de l'acheteur

Respect des exigences de sécurité de l'acheteur :

Au même titre que les agents de l'acheteur, le titulaire doit prendre connaissance et appliquer les règlements internes de l'acheteur (PSSI, directive d'utilisation des systèmes d'information, directive d'utilisation de la messagerie, etc.).

Respect des standards et méthodologies de l'acheteur :

Le titulaire doit respecter les standards et les méthodologies préconisés au sein de l'acheteur.

Respect du périmètre de la prestation :

Le titulaire ne tente pas d'accéder à des informations ou des ressources informatiques ne faisant pas partie du périmètre de la prestation.

Connexion d'équipements au réseau de l'acheteur :

Le titulaire doit connecter sur le réseau interne de l'acheteur uniquement des équipements fournis par l'acheteur. Cela comprend tout type de matériel y compris les supports de stockage amovibles (clés ou disques dur USB, etc.).

Inventaire des composants mis à disposition par l'acheteur :

Le titulaire met en place une solution pour élaborer et maintenir un inventaire complet et à jour des composants mis à disposition par l'acheteur. Cette liste devra être transmise régulièrement à l'acheteur.

Recensement des comptes d'accès :

Le titulaire tient à jour la liste exhaustive des comptes d'accès au SI de l'acheteur existants ainsi que des rôles et privilèges qui y sont associés.

Il doit être en mesure de fournir cette liste à l'acheteur sur demande.

Le titulaire doit également effectuer et formaliser une revue périodique* des comptes d'accès aux serveurs et autres ressources du titulaire utilisées dans le cadre de la Prestation.

*une revue « d'emploi » (a minima trimestrielle), une revue de « besoin » (a minima annuelle).

Restitution des équipements fournis par l'acheteur :

À la fin de la prestation, le titulaire doit restituer l'ensemble du matériel fourni par l'acheteur.

Restitution des informations collectées par le titulaire :

À la fin de la prestation, le titulaire doit restituer ou détruire les informations de l'acheteur en sa possession. Un procès-verbal de destruction des données doit être signé par le titulaire.

Transfert de connaissances :

Le titulaire doit préciser la date exacte de départ des intervenants de la prestation et organiser le transfert de connaissances auprès des équipes de l'acheteur.

11. Obligations relatives aux astreintes

Astreinte :

Le titulaire prévoit un dispositif garantissant les services d'astreinte nécessaires à la continuité de service et à la tenue des engagements. Les cas de force majeure doivent également être couverts.

Sécurisation des flux d'astreinte :

Le titulaire met en œuvre un tunnel sécurisé avec chiffrement des communications (ex. VPN, IPSec) pour la connexion à distance en astreinte aux réseaux utilisés dans le cadre de la Prestation (que ce soient ceux du titulaire, ceux de l'acheteur ou les deux éventuellement). Le personnel du titulaire devra explicitement lancer la connexion et s'authentifier pour obtenir l'accès aux SI à distance (connexion authentifiée non permanente) ou utiliser les services d'accès distants mis à disposition par l'acheteur.

Chiffrement des postes d'astreinte :

Le titulaire met en œuvre le chiffrement intégral du poste de travail utilisé en astreinte.

Authentification forte :

Le titulaire rend obligatoire l'utilisation de l'authentification forte (ex. badge, token) au poste de travail utilisé en astreinte.

Connexion distante :

Le titulaire restreint la connexion distante aux personnels d'astreinte, aux horaires d'astreintes définis (ex. connexion non autorisée en horaires ouverts), et aux ressources nécessaires en astreinte uniquement.

Enregistrement des accès :

Dans le cas où l'acheteur autorise la Prise en Main À Distance (PMAD) de ses infrastructures, le titulaire enregistre et sécurise les accès distants au SI de l'acheteur.

Suivi des interventions :

Le titulaire est capable de fournir à l'acheteur, sur demande, la liste de son personnel avec son nom, prénom et adresse mail, qui est intervenu à un instant donné sur le SI de l'acheteur en astreinte.

N.B : pour l'ensemble des interventions réalisées généralement hors heures ouvrées, l'acheteur assurera une tolérance d'accessibilité au SI de production à partir d'un site externe au lieu normal d'exécution de la mission. Toutefois, les agissants devront être spécialement identifiés et disposer d'une formation/sensibilisation conforme aux attentes de sécurité.

12. Obligations relatives à l'interconnexion entre les SI de l'acheteur et du titulaire

Respect des exigences de sécurité de l'acheteur :

Au même titre que les agents de l'acheteur, le titulaire prend connaissance et applique les règlements internes de l'acheteur (PSSI, directive d'utilisation des systèmes d'information, directive d'utilisation de la messagerie, etc.).

Respect des standards et méthodologies de l'acheteur :

Le titulaire respecte les standards et les méthodologies préconisés au sein de l'acheteur et figurant en annexe du présent CCTP.

Respect du périmètre de la prestation :

Le titulaire ne doit pas tenter d'accéder à des informations ou des ressources informatiques ne faisant pas partie du périmètre de la prestation.

Interconnexion des SI de l'acheteur et du titulaire :

En cas d'interconnexion des SI de l'acheteur et du titulaire, le titulaire doit prendre les mesures de sécurité nécessaires afin de maintenir le niveau de sécurité global des SI. L'interconnexion devra être réalisée via des infrastructures d'accès validées par l'acheteur au travers d'une étude ciblée, dans le respect du cadre technique et des règles de sécurité de l'acheteur.

Pour chaque interconnexion, les éléments suivants doivent être définis :

- les flux et protocoles autorisés, ainsi que les ressources auxquelles le titulaire est autorisé à accéder au travers de la zone « partenaires ». Ces éléments doivent être restreints au strict nécessaire ;
- les modalités d'authentification requises : authentification par mot de passe, authentification forte par mot de passe unique ou par certificat ;
- les modalités de chiffrement des échanges : le chiffrement des flux transitant sur Internet est requis ;
- les exigences spécifiques de traçabilité des accès ;
- les moyens de sécurité supplémentaires à mettre en œuvre : contrôle de conformité, outils de détection ou de prévention d'intrusion, contrôle de contenu, filtrage applicatif...

13. Prestations d'achat de matériels/logiciels

Absence de failles à la mise en production :

le titulaire s'engage à ce que les produits du contrat soient, au jour de leur mise en production pour l'acheteur, dépourvus de toute faille, faiblesse ou défaut de conception portant atteinte à la sécurité des informations.

Détection d'une vulnérabilité :

En cas de mise en évidence d'une vulnérabilité affectant un produit du contrat, le titulaire doit mettre à disposition de l'acheteur dans les meilleurs délais une solution de contournement ou une solution palliative (mise à disposition de correctifs) n'affectant ni les performances ni les fonctionnalités du produit concerné.

Le titulaire collabore également avec l'acheteur pour déterminer l'origine de la vulnérabilité et les actions à engager pour l'éradiquer.

Exigences liées à la maintenance :

Dans le cadre d'une opération de maintenance, le titulaire s'engage à chiffrer ou effacer de manière sécurisée toutes les données avant l'envoi en maintenance externe de toute ressource informatique de l'acheteur.

Si les données ne sont pas sensibles, et si elles ne peuvent être chiffrées ou effacées en totalité (par exemple : disque dur défectueux sous garantie), l'envoi en maintenance externe ne peut se faire que sous couvert d'un engagement de confidentialité de la part du mainteneur, ou bien dans le cadre d'une réparation sur site en présence d'un membre de l'équipe locale chargée des systèmes d'information.

Si les données sont sensibles et si elles ne peuvent être chiffrées ou effacées en totalité, l'envoi en maintenance externe est interdit.

Exigences liées à la télémaintenance :

Dans le cadre d'un accès de télémaintenance à une ressource informatique (matériel, logiciel) de l'acheteur, le titulaire doit présenter des mesures de sécurité renforcées validées par l'acheteur.

Exigences liées à la qualification :

En cas d'achat de produits de sécurité qualifiés, il est nécessaire de se référer au guide d'achat des produits qualifiés de l'ANSSI. Si le produit vise une qualification après la notification du marché, il est fortement recommandé que le jalon J0 du processus de qualification soit franchi préalablement.

Exemples de mesures de sécurité renforcées :

- Mise au rebut : pour tout départ définitif d'un matériel ou logiciel du service, le titulaire doit empêcher de manière sécurisée l'accès aux données présentes sur les disques durs ou dans la mémoire intégrée. Un procès-verbal doit être signé entre le titulaire et l'acheteur.

En cas d'impossibilité de réaliser un effacement sécurisé sur tout ou partie des disques ou de la mémoire (par exemple pour raison de panne ou dysfonctionnement), le disque dur ou la mémoire doit être détruit(e) physiquement avant de quitter définitivement le service ou démonté(e) et entreposé(e) sur site dans un local sécurisé en attente de destruction.