RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

RÉSEAU DE FORMATION DES ENSEIGNANTS

Marché n° 26-024
Datacenter
Hébergement & Liaisons

CAHIER DES CLAUSES TECHNIQUES PARTICULIERES

ANNEXE 1

SECURITE DES SYSTEMES D'INFORMATION

Table des matières

ARTICLE 1. Etat de l'art 7
1.1. Interfaces web 7
1.2. Services de courriels 7
ARTICLE 2. Caractéristique(s) particulière(s) des prestations 7
ARTICLE 3. Politique, organisation et gouvernance de la sécurité 7
3.1. Politique de sécurité du titulaire 7
3.2. Organisation de la sécurité adéquate 8
3.3. Existence d'un correspondant de sécurité 8
3.4. Mise en œuvre d'une gestion de risques et son suivi 8
3.5. Gestion de crise sécurité 8
3.6. Audit de sécurité 9
3.7. Réversibilité et transférabilité 9
ARTICLE 4. Gestion des biens 9
4.1. Séparation des données de l'acheteur et des données d'autres clients 9
4.2. Protection de la documentation de l'acheteur sur support papier 9
4.3. Modalités d'échanges d'informations 9
4.4. Échange de supports 9
4.5. Transmission de fichiers sur un support physique 10
4.6. Marquage des ressources techniques 10
4.7. Supports de stockage hébergeant des données de l'acheteur 10
4.8. Maintien à jour et mise à disposition des données relatives à la prestation 10
4.9. Destruction des données 10
ARTICLE 5. Sécurité des réseaux et de l'exploitation 10
5.1. Cloisonnement des environnements informatiques 10
5.2. Sécurisation des flux d'administration 10
5.3. Règles de sécurité et d'exploitation 11
5.4. Anti-virus opérationnel et à jour 11
5.5. Gestion des mises à jour 11
5.6. Sauvegarde des données 11
5.7. Stockage des sauvegardes informatiques 11
5.8. Comptes individuels 11
5.9. Comptes obsolètes ou par défaut 11
5.10. Comptes techniques 11
5.11. Recensement des comptes d'accès 12

5.12. Politique du moindre privilège 12
5.13. Attaques en essai et erreurs sur secrets d'authentification 12
5.14. Journalisation des actions 12
5.15. Gestion des traces 12
5.16. Politique de mot de passe 12
5.17. Sources d'installation des logiciels 13
5.18. Validité des licences 13
5.19. Traitement des obsolescences 13
5.20. Correctifs de sécurité 13
5.21. Cartographie des systèmes d'information 13
5.22. Mise à disposition des documents relatifs aux politiques et procédures de sécurité 13
ARTICLE 6. Sécurité du poste de travail 13
6.1. Protection contre le vol des postes de travail 13
6.2. Chiffrement du poste de travail 14
ARTICLE 7. Traitement des incidents 14
7.1. Remontée d'alerte 14
7.2. Enregistrement et traçabilité et gestion des incidents de sécurité 14
7.3. Traitement des incidents de sécurité 14
7.4. Base de connaissance 14
ARTICLE 8. Disponibilité des données et des systèmes d'information 14
ARTICLE 9. Continuité des services 14
9.1. Plan de continuité d'activité 14
9.2. Remplacement du matériel endommagé ou perdu 15
9.3. Incident affectant la continuité des services 15
ARTICLE 10. Conformité, audit, inspection, contrôle 15
10.1. Autocontrôles de sécurité 15
10.2. Régularisation des écarts ou des non-conformités au niveau d'exigence de sécurité de l'acheteur 15
ARTICLE 11. Obligations relatives à l'intervention du titulaire dans les locaux de l'acheteur 15
11.1. Respect des exigences de sécurité de l'acheteur 15
11.2. Respect des standards et méthodologies de l'acheteur 15
11.3. Respect du périmètre de la prestation 15
11.4. Connexion d'équipements au réseau de l'acheteur 15
11.5. Inventaire des composants mis à disposition par l'acheteur 16
11.6. Recensement des comptes d'accès 16
11.7. Restitution des équipements fournis par l'acheteur 16
11.8. Restitution des informations collectées par le titulaire 16
11.9. Transfert de connaissances 16

ARTICLE 12. Obligations relatives aux astreintes 16
12.1. Astreinte 16
12.2. Sécurisation des flux d'astreinte 16
12.3. Chiffrement des postes d'astreinte 16
12.4. Authentification forte 17
12.5. Enregistrement des accès 17
12.6. Suivi des interventions 17
ARTICLE 13. Obligations relatives à l'interconnexion entre les SI de l'acheteur et du titulaire 17
13.1. Respect des exigences de sécurité de l'acheteur 17
13.2. Respect des standards et méthodologies de l'acheteur 17
13.3. Respect du périmètre de la prestation 17
13.4. Interconnexion des SI de l'acheteur et du titulaire 17
ARTICLE 14. Obligations spécifiques liées aux prestations d'étude 18
14.1. Respect des standards et méthodologies de l'acheteur 18
14.2. Ségrégation des environnements 18
14.3. Conduite des tests 18
ARTICLE 15. Obligations spécifiques liées aux prestations de développement 18
15.1. Utilisation du cadre de cohérence technique de développement 18
15.2. Ségrégation des environnements 18
15.3. Protection des codes sources 18
15.4. Documentation du code 18
ARTICLE 16. Obligations spécifiques liées aux prestations d'hébergement 19
16.1. Respect de la directive de sécurité de l'hébergement informatique de l'acheteur 19
16.2. Changement de localisation géographique des services et des données 19
16.3. Hébergement de données 19
16.4. Contrôle d'accès physique aux bâtiments du titulaire 19
16.5. Contrôle des accès aux ressources techniques du titulaire 19
16.6. Protection intrusion physique des locaux techniques du titulaire 19
16.7. Accompagnement des visiteurs 19
16.8. Protection des plateaux mutualisés 20
16.9. Étanchéité physique des ressources informatiques 20
ARTICLE 17. Obligations spécifiques liées aux prestations d'achats de matériel et/ou logiciels 20
17.1. Absence de failles à la mise en production 20
17.2. Détection d'une vulnérabilité 20
17.3. Exigences liées à la maintenance 20
17.4. Exigences liées à la télémaintenance 21
ARTICLE 18. Evaluation de la conformité du titulaire aux exigences et préconisations de l'acheteur 21

Objet du marché / Clauses du CCTP	Prestations intellectuelles (études, conseil, audit, etc.)	Hébergement externe dont logiciels en Saas	Achat de matériels et logiciels	Exploitation et supervision	Etudes et développement
Etat de l'art (§ 1	☑	☑	☑	☑	☑
Caractéristique(s) particulière(s) des prestations (§ 2)	☑	☑	☑	☑	☑
Politique, organisation et gouvernance de la sécurité (§ 3)		☑		☑	☑
Gestion des biens (§ 4)	☑	☑	☑	☑	☑
Sécurité des réseaux et de l'exploitation (§ 5)		☑		☑	☑
Sécurité des postes de travail (§ 6)	☑	☑	☑	☑	☑
Traitement des incidents (§ 7)		☑		☑	
Disponibilité des données et des systèmes d'information (§ 8)		☑		☑	
Continuité des services (§ 9)		☑		☑	
Conformité, audit, inspection, contrôle (§ 10)	☑	☑		☑	☑
Obligations pour les titulaires intervenant au sein des locaux de l'acheteur (§ 11)	☑			☑	☑
Obligations pour les titulaires intervenants en situation d'astreinte (§ 12)		☑		☑	
Obligations en cas d'interconnexion entre les SI de l'acheteur et du titulaire (§ 13)		☑		☑	☑
Clauses d'études (§ 14)					
Clauses de développement (§ 15)					☑
Clauses d'hébergement (§ 16)		☑			
Clauses d'achat de matériels/logiciels (§ 17)			☑		

ARTICLE 1. Etat de l'art

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.

1.1. Interfaces web

- les développements ne doivent pas générer d'adhérence avec des modules spécifiques (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 du mécanisme de sécurité HSTS est obligatoire;
- 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.

1.2. Services de courriels

- les mécanismes de chiffrement TLS (dans des versions non obsolètes) 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)).

ARTICLE 2. Caractéristique(s) particulière(s) des prestations

Des spécifications techniques particulières ou des labels peuvent être exigés dans le cadre de certaines prestations. Dans ce cas, elles sont décrites et détaillées dans le CCTP. Le titulaire présente les certificats, attestations et visas de sécurité qui permettent de vérifier l'adéquation de la réponse à l'exigence du CCTP.

ARTICLE 3. Politique, organisation et gouvernance de la sécurité

3.1. Politique de sécurité du titulaire

Pour certaines prestations, l'acheteur exige la formalisation d'un PAS (Plan Assurance Sécurité). Le titulaire propose dans sa réponse un modèle de PAS. Sinon, le document type de Réseau Canopé s'applique (Cadre de réponse – plan d'assurance sécurité).

Le PAS de la prestation est rédigé entre les parties, notamment si le contexte du projet concerne des informations stratégiques, nominatives ou confidentielles.

Exigence : Le titulaire applique et fait appliquer à ses sous-traitants la politique de sécurité du présent marché constituée de la présente annexe et du PAS rédigé le cas échéant dans le cadre de l'exécution de sa prestation.
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.

3.2. Organisation de la sécurité adéquate

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

3.3. Existence d'un correspondant de sécurité

Exigence : 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 ; (Chargé du maintien et de la mise en application du PAS.)
- ce correspondant est joignable selon les horaires définis dans le CCTP. Tout remplacement de ce correspondant doit être notifié à l'acheteur conformément à l'article correspondant du CCAP concernant le remplacement du personnel. De plus, une suppléance de ce correspondant de sécurité doit être assurée pour pallier son indisponibilité.

3.4. Mise en œuvre d'une gestion de risques et son suivi

Exigence : 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.

3.5. Gestion de crise sécurité

Exigence : Sur son domaine de responsabilité SI, le titulaire applique un 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).

3.6. Audit de sécurité

Exigence : L'acheteur peut effectuer ou de faire effectuer un audit de sécurité auprès du titulaire ou le cas échéant de ses sous-traitants afin de s'assurer de la prise en compte effective du niveau de sécurité requis par l'acheteur.
Le titulaire est informé 15 jours à l'avance (date de l'audit, modalités financières pour l'acheteur et le titulaire, etc.).
L'acheteur, ou l'organisme mandaté à cette fin, peut, pendant une période de six mois à compter de la fin ou de la résiliation du marché, exercer un contrôle dans les locaux du titulaire et, le cas échéant, dans ceux de ses sous-traitants afin de vérifier que les dispositions en matière de destruction des données ont été effectivement appliquées.

3.7. Réversibilité et transférabilité

Exigence : Le titulaire met en œuvre des mesures techniques et organisationnelles pour garantir la sécurité des données et des applications qui lui sont confiées, lors du transfert des prestations de la part du précédent titulaire en conformité avec les réglementations applicables.
Durant la phase de transfert, l'assurance de la sécurité réside notamment dans :
- la gestion des accès, habilitations ;
- le transfert de responsabilités ;
- la fourniture d'informations nécessitant des mesures de protection adaptées ;
- la gestion de la continuité de l'activité.

ARTICLE 4. Gestion des biens

4.1. Séparation des données de l'acheteur et des données d'autres clients

Exigence : 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.

4.2. Protection de la documentation de l'acheteur sur support papier

Exigence : 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.

4.3. Modalités d'échanges d'informations

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

4.4. Échange de supports

Exigence : Le titulaire s'assure que les supports échangés ou à connecter sur un SI de l'acheteur n'intègrent aucun code malveillant.

4.5. Transmission de fichiers sur un support physique

Exigence : 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.
Préconisation : 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.

4.6. Marquage des ressources techniques

Préconisation : 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.

4.7. Supports de stockage hébergeant des données de l'acheteur

Exigence : 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.

4.8. Maintien à jour et mise à disposition des données relatives à la prestation

Exigence : 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.

4.9. Destruction des données

Exigence : Au terme du marché ou en cas de résiliation, le titulaire restitue sans délai à l'acheteur une copie de l'intégralité des données confiées par lui dans le cadre de la prestation. Une fois la restitution effectuée, le titulaire doit détruire, dans un délai de (à compléter), les éventuelles copies de données détenues dans son système d'information, y compris les données ayant fait l'objet de sauvegardes ou d'un archivage. La restitution et la destruction des données seront constatées par un procès-verbal daté et signé par le titulaire.

ARTICLE 5. Sécurité des réseaux et de l'exploitation

5.1. Cloisonnement des environnements informatiques

Exigence : Le titulaire est garant du bon cloisonnement (physique ou logique) des environnements utilisés dans le cadre de la prestation.

5.2. Sécurisation des flux d'administration

Exigence : Le titulaire chiffre tous les flux d'administration (système et fonctionnelle) par des procédés fiables garantissant la confidentialité et l'intégrité des données. Par ailleurs, les postes

d'administration utilisés pour la prestation doivent être dédiés et n'avoir accès ni à Internet, ni à aux infrastructures bureautiques du titulaire.

5.3. Règles de sécurité et d'exploitation

Exigence : L'installation, l'exploitation et l'administration des moyens mis en œuvre dans le cadre des prestations sont conformes aux bonnes pratiques et aux règles de sécurité et d'exploitation établies par l'acheteur. Toute exception fait l'objet d'un accord préalable écrit des équipes de l'acheteur.

5.4. Anti-virus opérationnel et à jour

Exigence : Le titulaire s'assure de la bonne installation et mise à jour d'un logiciel anti-virus sur tous les postes de travail et serveurs dont il est responsable dans le cadre de la prestation.
La désactivation, même temporaire, d'un antivirus sur un serveur utilisé dans le cadre de la prestation doit être préalablement notifiée à l'acheteur.

5.5. Gestion des mises à jour

Exigence : Le titulaire gère les mises à jour et l'application des correctifs de sécurité et des mises à jour antivirales, pour assurer le maintien en condition opérationnelle de l'ensemble de ses équipements pour les services fournis à l'acheteur.

5.6. Sauvegarde des données

Exigence : Le titulaire met en place un système de sauvegarde permettant la sauvegarde des données hébergées sur les serveurs du titulaire conformément aux besoins de sauvegarde exprimés dans le CCTP.
Des tests périodiques (a minima semestriels) de restauration des sauvegardes effectuées sur les données contenues dans les serveurs du titulaire sont formalisés et effectués.

5.7. Stockage des sauvegardes informatiques

Exigence : Le titulaire protège les sauvegardes informatiques en les stockant dans un coffre étanche et ignifuge pour les supports magnétiques, ou sur un site de back up sécurisé.

5.8. Comptes individuels

Exigence : Le titulaire s'assure que son personnel devant accéder à des ressources informatiques ou réseau dans le cadre de la prestation (qu'elles soient hébergées chez le titulaire ou chez l'acheteur) dispose d'un compte individuel qui peut être :

- soit un compte nominatif qui lui est personnel et qui est utilisé uniquement par cette personne tout au cours de la vie du compte ;
- soit un compte individualisé qui peut être attribué à des personnes différentes au cours de la vie du compte tout en n'étant toujours attribué qu'à une seule personne à la fois.

5.9. Comptes obsolètes ou par défaut

Exigence : Le titulaire s'assure de la suppression de tous les comptes inutiles ou obsolètes. De même, les mots de passe par défaut d'usine doivent être systématiquement modifiés.

5.10. Comptes techniques

Exigence : Dans le cadre de la cartographie des comptes d'administration du système d'information de l'établissement, le titulaire doit fournir un inventaire justifié des comptes

techniques (le compte propriétaire du fichier de la base de données, des données du serveur WEB, ...) nécessaires au fonctionnement du système.

5.11. Recensement des comptes d'accès

Exigence : 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 fournit cette liste à l'acheteur sur demande.
Le titulaire effectue et formalise 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 » (à minima trimestrielle) et une revue de « besoin » (à minima annuelle).

5.12. Politique du moindre privilège

Exigence : Le titulaire s'assure que tous les comptes (accès Windows et autres...) des intervenants dans le cadre de la prestation sont habilités selon le principe du moindre privilège.

5.13. Attaques en essai et erreurs sur secrets d'authentification

Exigence : Les moyens d'authentification mis en place par le titulaire (sur ses serveurs, applications et postes de travail) incluent une protection contre les attaques en essai et erreur sur les secrets d'authentification.

5.14. Journalisation des actions

Exigence : Le titulaire conserve de manière exploitable, sur une durée d'un an après la fin de la prestation, la trace des actions réalisées dans son système à des fins de contrôle (audit) et de preuves.
Le titulaire collecte et stocke à minima les informations suivantes :

- connexion et déconnexion aux équipements et applications ;
- consultations d'informations relatives à la vie privée ;
- informations d'usage de l'Internet (accès aux sites Web) ;
- accès en lecture et/ou en écriture à des fichiers et dossiers marqués « CONFIDENTIEL » ;
- informations concernant les accès fructueux et infructueux (identifiant de l'utilisateur, date, heure) aux serveurs du titulaire.

Les traces enregistrées par le titulaire doivent être imputables à un individu, elles sont par ailleurs horodatées selon une référence horaire commune à l'ensemble des équipements d'un même réseau.

5.15. Gestion des traces

Préconisation : Le titulaire prévoit dans sa procédure de traitement d'incident un chapitre sur la préservation des traces éphémères (volatiles) en cas de suspicion d'attaque. Une trace volatile est une trace potentiellement utile pour l'analyse forensique d'une attaque informatique mais qui ne peut pas, par nature, être journalisée (contenu de la RAM, du swap, journal des transactions d'un système de fichier, divers dates liées aux fichiers, clés de registres...). La procédure établit comment limiter l'activité susceptible de détruire ces traces éphémères.

5.16. Politique de mot de passe

Exigence : Le titulaire respecte la politique de définition des mots de passe de l'acheteur sur l'ensemble des comptes d'accès utilisateurs aux postes de travail et applications sous la responsabilité du titulaire.

5.17. Sources d'installation des logiciels

Exigence : Le titulaire dispose des sources d'installation des logiciels utilisés dans le cadre de la prestation, lorsque ces logiciels ne sont pas mis à disposition par l'acheteur.

5.18. Validité des licences

Exigence : Le titulaire s'assure de la bonne validité des licences des logiciels qu'il met à disposition de son personnel ou de l'acheteur dans le cadre de la prestation.

5.19. Traitement des obsolescences

Exigence : Le titulaire doit n'utiliser que des composants logiciels que l'éditeur s'engage à maintenir pendant la durée du marché. Si la durée du marché dépasse la durée pendant laquelle un éditeur s'engage à maintenir un composant logiciel, le titulaire maintient, livre et respecte une feuille de route de migration vers des systèmes maintenus.

5.20. Correctifs de sécurité

Une vérification d'aptitude ou une vérification de service régulier (VA et VSR) peut être refusée si des composants ne sont pas à jours des correctifs de failles de sécurité publiés depuis un délai supérieur à [seuil à définir par l'acheteur].
L'acheteur définit les fréquences des livraisons en coordination avec les équipes d'exploitation, en fonction des différentes criticités des vulnérabilités concernées.
Le titulaire s'assure que l'application des correctifs de sécurité ne modifie pas les performances du système, en modifiant si besoin et à ses frais le système pour maintenir le niveau de performance malgré l'application du correctif

5.21. Cartographie des systèmes d'information

Le titulaire dispose d'un inventaire et d'une cartographie des systèmes d'information dont il a la charge et doit les maintenir, selon les préconisations de l'ANSSI[1] issues du guide « cartographie des systèmes d'information », dans l'outil mis à sa disposition par l'acheteur. L'inventaire et la cartographie comprennent également la liste des « briques » matérielles et logicielles utilisées, ainsi que leurs versions exactes avec leur configuration. Ils comportent une base de données de configuration. La cartographie est livrée à la demande de l'acheteur et au minimum [fréquence à définir par l'acheteur : un an est raisonnable].

5.22. Mise à disposition des documents relatifs aux politiques et procédures de sécurité

Exigence : Le titulaire met à disposition de l'acheteur l'ensemble des documents relatifs aux politiques et procédures de sécurité à la demande de l'acheteur.

ARTICLE 6. Sécurité du poste de travail

6.1. Protection contre le vol des postes de travail

Préconisation : 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.

[1] https://www.ssi.gouv.fr/guide/cartographie-du-systeme-dinformation/

6.2. Chiffrement du poste de travail

Préconisation : 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.

ARTICLE 7. Traitement des incidents

7.1. Remontée d'alerte

Exigence : 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).

7.2. Enregistrement et traçabilité et gestion des incidents de sécurité

Exigence : 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.

7.3. Traitement des incidents de sécurité

Exigence : 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 concerné par la prestation, le titulaire participe à la demande de l'acheteur au traitement de l'incident ;
- si cet incident a lieu sur le SI du titulaire, le titulaire autorise 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 sont planifiées avec l'acheteur (traitement des causes profondes).

7.4. Base de connaissance

Préconisation : 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.

ARTICLE 8. Disponibilité des données et des systèmes d'information

Exigence : 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 le délai maximum précisé dans le CCTP.
En cas de non-respect de ces délais, l'acheteur applique les pénalités visées dans le CCAP du marché ou par défaut dans le CCAG-TIC.

ARTICLE 9. Continuité des services

9.1. Plan de continuité d'activité

Ce paragraphe ne s'applique que si le CCTP du marché prévoit explicitement un plan de continuité d'activité.
Exigence : Le titulaire assure la disponibilité de l'ensemble des services liés à la prestation tout au long du contrat. Les délais maxima d'indisponibilité sont précisés dans le CCTP. Il fournit, à la demande de l'acheteur, la preuve de l'existence d'un plan de continuité d'activité régulièrement testé pour l'ensemble des services fournis à l'acheteur.

L'acheteur se réserve le droit de demander les résultats des exercices de continuité d'activité réalisés régulièrement par le titulaire.

9.2. Remplacement du matériel endommagé ou perdu

Exigence : 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).

9.3. Incident affectant la continuité des services

Exigence : En cas d'incident affectant la continuité des services, le titulaire signale l'événement à l'acheteur selon la procédure d'alerte définie entre les parties.

ARTICLE 10. Conformité, audit, inspection, contrôle

10.1. Autocontrôles de sécurité

Préconisation : Le titulaire effectue des autocontrôles de conformité aux exigences du PAS ou à défaut du CCTP pour garantir le niveau de sécurité au démarrage de la prestation ainsi que son maintien tout au long de la prestation.

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

Exigence : En cas de constatation d'écarts avec le PAS (s'il a été formalisé) et, plus généralement, en cas de non-conformité au niveau d'exigence de sécurité requis par l'acheteur, un plan de remédiation est 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.

ARTICLE 11. Obligations relatives à l'intervention du titulaire dans les locaux de l'acheteur

11.1. Respect des exigences de sécurité de l'acheteur

Exigence : Au même titre que les agents de l'acheteur, le titulaire doit prendre connaissance et appliquer les règlements internes de l'acheteur (PSSI, charte des bons usages des moyens numériques, charte administrateurs).

11.2. Respect des standards et méthodologies de l'acheteur

Préconisation : Le titulaire respecte les standards et les méthodologies préconisés au sein de l'acheteur et figurant dans le CCTP.

11.3. Respect du périmètre de la prestation

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

11.4. Connexion d'équipements au réseau de l'acheteur

Exigence : 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.)

11.5. Inventaire des composants mis à disposition par l'acheteur

Préconisation : 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 est transmise régulièrement à l'acheteur.

11.6. Recensement des comptes d'accès

Exigence : Le titulaire tient à jour la liste exhaustive des comptes d'accès au SI de l'acheteur nécessaires lors des interventions physiques ainsi que des rôles et privilèges qui y sont associés.
Il fournit cette liste à l'acheteur sur demande.

11.7. Restitution des équipements fournis par l'acheteur

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

11.8. Restitution des informations collectées par le titulaire

Exigence : A la fin de la prestation, le titulaire doit restituer ou détruire les informations de l'acheteur en sa possession.

Préconisation : Un procès-verbal de destruction des données doit être signé par le titulaire.

11.9. Transfert de connaissances

Exigence : 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.

ARTICLE 12. Obligations relatives aux astreintes

Ce paragraphe ne s'applique que si le CCTP du marché prévoit explicitement un dispositif d'astreinte.

12.1. Astreinte

Exigence : 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.

12.2. Sécurisation des flux d'astreinte

Exigence : 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 doit 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.

12.3. Chiffrement des postes d'astreinte

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

12.4. Authentification forte

Exigence : 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 ouvrés), et aux ressources nécessaires en astreinte uniquement.

12.5. Enregistrement des accès

Exigence : 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.

12.6. Suivi des interventions

Exigence : 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.

ARTICLE 13. Obligations relatives à l'interconnexion entre les SI de l'acheteur et du titulaire

13.1. Respect des exigences de sécurité de l'acheteur

Exigence : Au même titre que les agents de l'acheteur, le titulaire doit prendre connaissance et appliquer les règlements internes de l'acheteur (PSSI, charte des bons usages des moyens numériques, charte administrateurs).

13.2. Respect des standards et méthodologies de l'acheteur

Préconisation : Le titulaire respecte les standards et les méthodologies préconisés au sein de l'acheteur et figurant dans le CCTP.

13.3. Respect du périmètre de la prestation

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

13.4. Interconnexion des SI de l'acheteur et du titulaire

Exigence : 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 doit 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…

ARTICLE 14. Obligations spécifiques liées aux prestations d'étude

14.1. Respect des standards et méthodologies de l'acheteur

Exigence : Le titulaire doit respecter les standards et les méthodologies préconisés au sein de l'acheteur. En particulier, le titulaire doit appliquer les méthodes d'évaluation de la sensibilité et d'analyse de risques des systèmes d'information lorsqu'il intervient dans les phases amont des projets.

14.2. Ségrégation des environnements

Exigence : Le titulaire doit utiliser différents environnements cloisonnés pour les activités de développement, de recette et de pré-production.

14.3. Conduite des tests

Exigence : Lors de la conduite de tests de validation ou du déploiement, le titulaire doit :

- utiliser des données de tests anonymisées (sauf accord explicite de l'acheteur) ;
- ne pas provoquer de perturbations du système d'information de l'acheteur lors des séances de test ;
- remettre en l'état initial les systèmes testés et réinitialiser le matériel sensible.

ARTICLE 15. Obligations spécifiques liées aux prestations de développement

Réseau Canopé est doté d'un cadre de cohérence technique, précisant le cadre d'intervention général des prestataires, qui doit être appliqué pour tout développement.

15.1. Utilisation du cadre de cohérence technique de développement

Le titulaire doit utiliser le cadre commun de développement (méthodes, démarches, etc.) de l'acheteur comprenant notamment :

- l'organisation des équipes de développement et de la prestation ;
- les configurations matérielles préconisées pour le développement ;
- les outils de développement préconisés par l'acheteur (logiciels, versions, etc.) ;
- une structure de développement (framework) intégrant les fonctions de sécurité.

15.2. Ségrégation des environnements

Le titulaire doit utiliser différents environnements cloisonnés pour les activités de développement, de recette (et si demandés, de pré-production).

15.3. Protection des codes sources

Le titulaire doit mettre en œuvre les mesures de sécurité nécessaires et adéquates à la protection des codes sources.

15.4. Documentation du code

Le titulaire doit commenter et documenter le code développé dans le cadre de la prestation selon les bonnes pratiques observées par la profession (code source, forge de développement, wiki,...). La documentation doit être mise à jour régulièrement.

ARTICLE 16. Obligations spécifiques liées aux prestations d'hébergement

16.1. Respect de la directive de sécurité de l'hébergement informatique de l'acheteur

Le titulaire doit respecter les exigences de la directive de sécurité de l'hébergement informatique de l'acheteur.

16.2. Changement de localisation géographique des services et des données

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

16.3. Hébergement de données

Exigence : A 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.

16.4. Contrôle d'accès physique aux bâtiments du titulaire

Exigence : 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.

16.5. Contrôle des accès aux ressources techniques du titulaire

Exigence : 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.

16.6. Protection intrusion physique des locaux techniques du titulaire

Exigence : 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.

16.7. Accompagnement des visiteurs

Exigence : 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.

16.8. Protection des plateaux mutualisés

Exigence : 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.).

16.9. Étanchéité physique des ressources informatiques

Préconisation : 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.

Exigence : 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 :

- L'espace 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 multiclients, 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.

ARTICLE 17. Obligations spécifiques liées aux prestations d'achats de matériel et/ou logiciels

17.1. Absence de failles à la mise en production

Exigence : Le titulaire s'assure 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.

17.2. Détection d'une vulnérabilité

Exigence : 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.

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

17.3. Exigences liées à la maintenance

Exigence : 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.

17.4. Exigences liées à la télémaintenance

Exigence : 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.

ARTICLE 18. Evaluation de la conformité du titulaire aux exigences et préconisations de l'acheteur

En complément de son offre technique, le titulaire présente un document de synthèse sur la sécurité de son système d'information (PAS).
Il désigne dans ce document le correspondant sécurité demandé dans le paragraphe 3.3 du présent document.
En cas d'impossibilité de répondre favorablement à une des exigences listées dans ce document, il présente les mesures de contournement ou les solutions alternatives qu'il envisage pour assurer le niveau de sécurité exigé par l'acheteur.