

RAPPORT

Service Exploitation
et Sécurité

Pôle Équipements et
Systèmes

Septembre 2025

Dossier de Consultation des Entreprises

SAGACITE

**Annexe 7 – CCTP Sagacité - AMO & TMA–
Clauses de sécurité informatique**



**MINISTÈRE
CHARGÉ
DES TRANSPORTS**

*Liberté
Égalité
Fraternité*

**Direction interdépartementale
des routes Centre-Est**

www.dir-centre-est.fr

Historique des versions du document :

Version	Date	Commentaire
0.1	07/08/25	Version initiale

Affaire suivie par :

François ROCHAT- SES / PES
<i>Tel : +33 4 72 47 16 24 - Mobile : +33 6 62 42 54 77</i>
Courriel : francois.rochat@developpement-durable.gouv.fr

Jean-Philippe GUILLAUD - SES / PES
<i>Tél. : +33 4 72 47 16 13 Fax : +33 6 64 24 56 50</i>
Courriel : jean-philippe.guillaud@developpement-durable.gouv.fr

Rédacteur :

François ROCHAT - SES / PES

Relecteurs:

Jean-Philippe GUILLAUD - SES / PES
Pascal Glasson – SES / PES

Table des matières

1 - PRÉAMBULE.....	6
2 - DOCUMENTS DE RÉFÉRENCE.....	6
3 - OBLIGATIONS GÉNÉRALES DE SÉCURITÉ.....	7
3.1 - Transfert du système.....	7
3.2 - Responsabilité.....	7
3.2.1 - Obligations du maître d'ouvrage.....	7
3.2.2 - Obligations du titulaire.....	7
3.2.3 - Obligations du titulaire relatives aux astreintes et à la télémaintenance.....	8
3.3 - Suivi.....	8
3.4 - Confidentialité.....	9
3.5 - Localisation des données.....	9
3.6 - Convention de service.....	10
3.7 - Audit de sécurité.....	10
3.8 - Sécurité des développements applicatifs.....	11
3.9 - Gestion des évolutions.....	12
3.10 - Réversibilité.....	12
3.11 - Résiliation	13
4 - EXIGENCES DE SÉCURITÉ.....	14
4.1 - Gestion de la sécurité.....	14
4.2 - Traitement des incidents de sécurité.....	14
4.3 - Exigences relatives aux achats de matériel.....	14
4.3.1 - Vulnérabilités matérielles.....	15
4.3.2 - Fournisseurs tiers.....	15
4.3.3 - Logiciels embarqués.....	15
4.3.4 - Compatibilité avec les systèmes existants.....	15
4.4 - Connaître le Système d'Information.....	15
4.4.1 - État de l'art Connaître le Système d'Information.....	15
4.4.2 - Cartographie des systèmes.....	16
4.5 - Gestion des identités et des accès.....	16
4.5.1 - Authentification.....	16
4.5.2 - Contrôle des authentifications.....	17
4.5.3 - Inventorier les comptes utilisateurs et leur niveau de privilège.....	17
4.5.4 - Stockage sécurisé des mots de passe.....	18
4.6 - Gestion des flux.....	18

4.6.1 - Confidentialité et intégrité des flux.....	18
4.6.2 - Contrôle et filtrage des flux.....	19
4.6.3 - Protéger les expositions directes sur Internet.....	20
4.7 - Protection antivirale.....	20
4.8 - Gestion des mises à jour.....	20
4.8.1 - Mise à jour des correctifs de sécurité.....	20
4.8.2 - Cas particulier d'utilisation de systèmes obsolètes.....	21
4.9 - Sauvegarde et restauration.....	21
4.10 - Continuité de l'activité.....	22
4.11 - Imputabilité et traçabilité.....	22
4.12 - Durcissement des configurations.....	22
4.12.1 - Utilisation d'un système d'exploitation durci.....	22
4.12.2 - Restriction des collectes de données.....	23
4.12.3 - Restriction sur l'utilisation des supports amovibles.....	23
4.13 - Sécurisation des réseaux.....	23
4.13.1 - Réseaux Wifi.....	23
4.13.2 - Création ou extension de réseaux.....	24
4.14 - Sécuriser l'administration.....	25
4.14.1 - Utiliser les protocoles d'administration sécurisés.....	25
4.15 - Sécuriser les applications web.....	25
4.16 - Choix des composants du système.....	26
4.16.1 - Privilégier l'usage de produits qualifiés par l'ANSSI.....	26
4.17 - Journalisation.....	26
4.18 - Contrôle de la prise en compte de ces mesures avant le déploiement en production.....	27
4.19 - Personnels en charge des prestations.....	27
4.19.1 - Liste de personnels intervenant sur le SI.....	27
4.19.2 - Qualification et formation dans le domaine de la SSI.....	27
4.19.3 - Exigences de sécurité pour les personnels extérieurs.....	28
5 - EXIGENCES DE SÉCURITÉ SPÉCIFIQUES POUR LES SI HÉBERGÉS CHEZ LE TITULAIRE.....	28
5.1 - Sauvegarde et restauration.....	28
5.2 - Continuité de l'activité.....	29
5.2.1 - Mise à jour des correctifs de sécurité.....	29
5.3 - Protection des locaux.....	30
5.3.1 - Continuité des services essentiels : énergie, climatisation et télécommunications.....	30
5.3.2 - Protection contre les incendies.....	30
5.3.3 - Surveillance et contrôle des accès aux locaux de l'hébergeur, en particulier au local d'hébergement du système d'information	

.....31

5.3.4 - Intervention des sociétés de maintenance ou de support de solutions informatiques (matérielles ou logicielles).....31

6 - BONNES PRATIQUES POUR L'HÉBERGEMENT MUTUALISÉ.....32

6.1 - Journaux d'événements et conservation des traces.....32

6.2 - Suivi du service hébergé.....32

6.3 - Prévention d'une attaque.....33

6.4 - Réaction sur incident.....33

7 - ANNEXE 1 : EXEMPLE DE CLAUSES DE CONFIDENTIALITÉ TYPE EN CAS DE SOUS-TRAITANCE.....35

1 - Préambule

Ce document présente les exigences de sécurité à respecter par l'ensemble des projets s'intégrant dans le Système d'Information des DIR.

Ces exigences de sécurité sont inspirées du Guide d'hygiène informatique [DR01], du guide d'intégration de la sécurité dans les projets [DR12] et du guide d'externalisation des systèmes d'information de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI), et permettent de fixer les règles de protection minimales applicables à tout SI et donc également aux SI de l'État, par application de la Politique de Sécurité des SI de l'État (PSSIE) [DR02].

Dans la suite du document, les systèmes, applications ou matériels concernés par l'objet du marché pourront être regroupés sous la dénomination de système.

2 - Documents de référence

Exemple de documents de référence établis par l'ANSSI :

Réf.	Intitulé
JO RF n°0078 du 1 avril 2021 Texte n° 22	Cahier des clauses administratives générales des marchés publics de techniques de l'information et de la communication
Guides ANSSI accessibles sur le site de l'ANSSI « Publications »	• Architecture sécurisée de SI • Infrastructure de gestion des clés (IGC) • Zero Trust • Modèle Zéro Trust • Approche SSI pour l'internet des objets industriels • Sélection d'un logiciel libre • La cybersécurité des systèmes industriels • L'homologation de sécurité des systèmes d'information • Données et traitements sensibles • Se protéger des fuites de données • Automatisation de la gestion des certificats avec ACME • Recommandations relatives aux architectures des services DNS • Recommandations pour l'hébergement des SI sensibles dans le cloud • Sécurisation d'une infrastructure VMware • DevSecOps • Virtualisation • Recommandations pour l'administration sécurisée des SI reposant sur l'AD • Les mesures Cyber Préventives Prioritaires • Sauvegarde des systèmes d'information • Recommandations de sécurité pour l'architecture d'un système de journalisation • Sécuriser la journalisation dans un environnement Microsoft Active Directory • Recommandations relatives à l'authentification multifacteur et aux mots de passe

	• Recommandations pour la protection des systèmes d'information essentiels • Doctrine de détection pour les systèmes industriels • Exigences de sécurité matérielles • Recommandations de sécurité relatives à un système GNU/Linux • Cartographie du système d'information • Agilité et sécurité numériques : méthode et outils à l'usage des équipes projet • Guide d'hygiène informatique • La télé-assistance sécurisée • La cybersécurité des systèmes industriels : étude de cas d'un tunnel routier • Recommandations de sécurité pour les architectures basées sur VMware vSphere ESXi • Référentiel d'exigences de sécurité pour les prestataires d'intégration et de maintenance de systèmes industriels • Recommandations de sécurité concernant l'analyse des flux HTTPS • Usage sécurisé d'(Open)SSH • Sécuriser les accès Wi-Fi
--	--

3 - Obligations générales de sécurité

3.1 - Transfert du système

Le prestataire se porte garant de l'intégrité et de la confidentialité des données qui lui sont confiées pendant la phase de transfert du système d'information.

Lorsqu'il est évoqué le transfert de système, il s'agit notamment et spécifiquement le transfert de données, code, habilitations ou tout autres du système vers les plateformes de tests et inversement si le cas se présente.

Il appartient en particulier au prestataire de contrôler les sauvegardes des informations des DIR et de gérer ces sauvegardes de manière à permettre une reprise en cas d'incident lors de la bascule du système si nécessaire.

3.2 - Responsabilité

3.2.1 - Obligations du maître d'ouvrage

Le Maître d'Ouvrage s'engage à faire connaître au titulaire les anomalies qu'il est amené à constater, et ce, dans les meilleurs délais.

Il assure que toutes les interventions de maintenance n'étant pas du ressort du titulaire

seront effectuées dans les règles de l'art, de telle façon que cela ne provoque pas de pannes intempestives sur les matériels ou équipements faisant l'objet du présent marché.

Il permet au personnel du titulaire d'avoir accès aux installations, aux schémas, aux réglages... et lui communiquera toutes modifications quant à l'installation/suppression des matériels et équipements.

3.2.2 - Obligations du titulaire

Le prestataire reconnaît être tenu à une obligation de conseil, de mise en garde et de recommandations en termes de sécurité et de mise à l'état de l'art. En particulier il s'engage à informer les DIR des risques d'une opération envisagée, des incidents éventuels ou potentiels, et de la mise en œuvre éventuelle d'actions correctives ou de prévention.

Outre le respect de ses obligations au titre de la convention de service, le prestataire informera préalablement les membres du Groupement de toute opération susceptible de provoquer l'indisponibilité (ou une dégradation des performances) du système.

Le prestataire est responsable du maintien en condition de sécurité du système pendant toute la durée des prestations.

Les mécanismes de sécurité mis en œuvre doivent évoluer conformément à l'état de l'art : la découverte de failles dans un algorithme, un protocole, une implémentation logicielle ou matérielle, ou encore l'évolution des techniques de cryptanalyse et des capacités d'attaque par force brute doivent être pris en compte.

3.2.3 - Obligations du titulaire relatives aux astreintes et à la télémaintenance

- **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 utilisera uniquement le tunnel sécurisé avec chiffrement des communications (VPN certifié) mise à disposition de la DIR pour la connexion à distance, en astreinte ou en situation de télémaintenance, 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 utiliser les services d'accès distants mis à disposition par la DIR.
- **Chiffrement des postes d'astreinte** : le titulaire met en œuvre le chiffrement intégral du poste de travail utilisé en astreinte ou pour les opérations de télémaintenance.
- **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 ouvrés), et aux ressources nécessaires en astreinte uniquement.

3.3 - Suivi

Un suivi, traduit par un volet sécurité présenté lors des instances contractuelles, permettra de gérer la mise en place et l'évolution du volet sécurité de la prestation : respect du calendrier, conformité des prestations, respect de l'obligation de collaboration, validation des améliorations pour accroître la sécurité. Il traitera également des questions techniques touchant à la sécurité : collaboration dans la gestion des droits et la gestion des incidents, détection des anomalies et préconisation d'améliorations, exploitation des résultats des audits de contrôle des prestations sécurité.

Ce comité traitera également, si les prestations du marché le nécessitent, des obligations liées à la loi du 6 janvier 1978 relative à l'Informatique, aux fichiers et aux libertés : déclaration par la DIR auprès de la CNIL, communication des déclarations au prestataire, informations par le prestataire des modalités de gestion ou d'exploitation des applications et des modifications de celles-ci.

Le comité de suivi s'assurera également des conditions techniques et financières de transfert des moyens de sécurité matériels et logiciels mis en place, en cas de réversibilité de l'opération.

3.4 - Confidentialité

Le prestataire et ses sous-traitants ont une obligation de discrétion, de sécurité et de secret (conformément à l'article 10 du CCAG).

L'ensemble des intervenants du prestataire s'engage à assurer la confidentialité de l'intégralité des informations traitées dans le cadre de la prestation.

La divulgation des informations ne devra se faire qu'aux seules personnes ayant le besoin d'en connaître. La méthodologie, la documentation, les informations ou le savoir-faire provenant des DIR sont considérés comme confidentiels, et le titulaire ne peut les utiliser que pour l'accomplissement de la prestation. Les informations sensibles ou confidentielles et le système d'information utilisés par le prestataire doivent respecter l'ensemble des règles de l'instruction interministérielle n° 9011 relative aux mesures de protection des systèmes d'information traitant d'informations sensibles non-classifiées de défense de niveau Diffusion Restreinte (DR). En cas de manipulation d'informations sensibles classifiées, le prestataire s'engage à respecter l'instruction générale interministérielle n° 13002 sur la protection du secret de la défense. En cas de sous-traitance, toutes ces obligations s'appliquent également aux sous-traitants.

Le PAS identifie les données sensibles et les règles qui s'y appliquent.

3.5 - Localisation des données

Les lieux d'hébergement des données doivent satisfaire aux exigences de sécurité du donneur d'ordres et aux dispositions de la loi du 6 janvier 1978 modifiée, relative à la protection des données personnelles.

Le prestataire doit communiquer la liste de tous les lieux de stockage de données (site d'hébergement principal, site(s) de secours, etc.). Dans le cadre d'architectures distribuées, il est demandé au prestataire d'être en mesure de localiser, a posteriori, et non en permanence, le lieu de stockage des données, en particulier suite à un incident.

A ce jour SAGACITE est un système hébergé dans les DIR. A moyen terme et selon les évolutions du système cette clause s'appliquerait.

Les plateformes de développement ou de tests ne peuvent être déportées chez des hébergeurs dont l'entité juridique est gérée par un pays disposant de lois autorisant l'État à accéder aux données (ex. « Patriot Act » aux États-Unis). (*cf. Annexe 8 – CCTAG_TIC Article 5*)

L'hébergement sur le territoire national des données sensibles de la DIR est obligatoire sauf accord explicite de la DIR et dérogation dûment motivée.

Enfin, en cas de changement de localisation des données ou services, le prestataire s'engage à informer préalablement la DIR et de fournir une solution respectant les clauses édictées dans l'article 3.5. (*cf. Annexe 8 – CCTAG_TIC Article 3.5*)

3.6 - Convention de service

Les engagements de niveau de service (SLA) sont décrits dans la convention de service. Dans cette convention de service sera précisé les SLA proposés et les KPI en découlant.

Se référer au §CCTP qui traite des niveaux de service pour la maintenance des SI 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, sont indiqués dans le CCTP .

3.7 - Audit de sécurité

Conformément à l'article 24 (*cf. Annexe 8 – CCTAG_TIC Article 24*), la DIR peut réaliser ou faire réaliser, à tout moment, un audit de sécurité pour vérifier que les exigences de sécurité sont satisfaites par les dispositions prises par le prestataire.

N.B. : Cet dernier audit a été réalisé par la DIR Centre Est en juin 2025.

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).

En cas d'incident de sécurité nécessitant une intervention urgente, le délai de 15 jours prévu au CCAG (*cf. Annexe 8 – CCTAG_TIC Article 13*) pourra être réduit.

Dans le cas où des écarts entre le niveau de sécurité effectif et les exigences de sécurité exprimées dans le présent CCTP seraient constatés et ne feraient l'objet d'aucune contestation de la part du prestataire, la DIR se réserve le droit d'appliquer les pénalités de retard liées au délai de non mise en conformité, ce délai court à partir de la mise en demeure notifiée par la DIR jusqu'à la mise en conformité. (*cf. Annexe 8 – CCTAG_TIC Article 14*).

En cas de contestation par le prestataire, la DIR se réserve le droit de faire réaliser un audit de sécurité par une entreprise tierce. Dans le cas où les conclusions de l'audit iraient dans le sens du prestataire, ce dernier n'aurait à subir aucune charge liée au frais engagé par la DIR. Les éventuels non conformités restantes seront traitées dans le cadre des prestations du marché.

Si les écarts sont confirmés par le rapport d'audit de l'entreprise tierce, et que le prestataire est désigné responsable de cette situation, alors non seulement le prestataire devra se mettre en conformité avec les exigences de sécurité du présent CCTP, payer la prestation d'audit et subir des pénalités de retard calculées selon la formule du CCAP (*cf. Annexe 8 – CCTAG_TIC Article 14*).

3.8 - Sécurité des développements applicatifs

Le prestataire est tenu d'assurer la sécurité des développements conformément à l'état de l'art dans chacune des technologies mises en œuvre.

Voici une liste (non exhaustive) de règles applicables :

- environnement applicatif maintenu en tenant compte des recommandations
- d'application de correctifs par les éditeurs ;
- contrôle rigoureux des entrées utilisateurs ;

- sécurisation des accès aux fonctions d'administration ;
- installation du minimum de fonctions nécessaires lors de l'installation ;
- principe du moindre privilège ;
- utilisation interdite de mots de passe dans le code ;
- mise en œuvre d'une gestion efficace des erreurs.

Pour la mise en œuvre de technologies web, les développements pourront s'appuyer sur les recommandations de l'OWASP (Open Web Application Security Project).

La recette de l'application comprend une revue de code permettant de s'assurer d'une implémentation conforme aux exigences de sécurité. La correction d'éventuelles anomalies détectées lors de la revue de code sont à la charge du prestataire.

3.9 - Gestion des évolutions

Les évolutions fonctionnelles ou techniques ne doivent pas remettre en cause le respect des exigences de sécurité ou compromettre une éventuelle opération de réversibilité.

En cas d'évolution, le prestataire doit vérifier que sa mise en œuvre est conforme aux exigences contractuelles et en apporter la justification auprès du donneur d'ordres, avant validation par ce dernier.

3.10 - Réversibilité

A la fin du présent marché, quel qu'en soit sa cause, le titulaire s'engage, dans les 3 mois précédant la fin de la prestation, à assurer la réversibilité du service.

Il s'agira de transmettre l'ensemble des ressources et des compétences requises pour la poursuite du service. Au cours de la période de réversibilité, le titulaire continue à assurer les activités qui lui sont attribuées, sauf contrordre du commanditaire.

Durant la période de réversibilité, le titulaire doit permettre au commanditaire de prendre le relais, ou de le faire prendre par un tiers. Cette transition doit être effectuée dans les meilleures conditions et sans interruption du service en cours.

Les modalités détaillées seront proposées par le candidat, elles seront affinées et planifiées avec le commanditaire le moment venu.

Le prestataire s'engage à apporter l'assistance nécessaire durant la période de migration pour faciliter le transfert des moyens de sécurité matériels et logiciels, et la reprise de leur exploitation par la DIR, ou par un autre prestataire de service.

Le prestataire s'engage à garantir, lors du transfert, la sécurité des données et des applications qui lui ont été confiées, conformément à ses obligations.

En outre, la phase de réversibilité ne doit pas, en principe, modifier la qualité, les termes et les conditions des services fournis durant le contrat et définis dans le Service Level

Agreement (SLA).

En cas d'arrêt des prestations confiées au titulaire par le donneur d'ordres, l'ensemble des matériels, logiciels et documentations confiés au titulaire doivent être restitués. Le déménagement de cet ensemble des locaux du titulaire sera assuré aux frais du titulaire dans un délai maximum d'un mois après l'arrêt des prestations confiées au titulaire

La prestation de réversibilité est déclenchée par une commande spécifique du commanditaire.

La MOA se réserve le droit d'interrompre à tout moment la mission de réversibilité avant sa fin.

À la fin de l'exécution du présent marché, le titulaire est tenu :

- de transférer à l'équipe du futur titulaire les informations sur le contexte fonctionnel et technique de l'ensemble applicatif ainsi que sur les aspects de suivi du projet ;
- de préparer un support informatique défini par le donneur d'ordres contenant tous les éléments (documentations, programmes, chaînes de compilation...) gérés par le titulaire actuel et qui seront, à l'issue de cette prestation, placés sous la responsabilité du futur titulaire (cette mise à disposition devra être faite sous un format pouvant permettre au futur titulaire d'installer, le cas échéant, l'ensemble de ces éléments sur une plate-forme de son choix pour examen approfondi par celui-ci) ;
- d'assurer une formation fonctionnelle approfondie (du type formation utilisateur et administrateur) aux personnels du futur titulaire, avec travaux pratiques sur poste de travail, en présence de représentants du donneur d'ordres. Cette formation devra s'appuyer sur les documentations utilisateurs et techniques rédigées par le titulaire.

En particulier, au titre de cette prestation, le titulaire :

- lance la prestation avec le futur titulaire et les représentants du donneur d'ordres. Il s'agit, au plus, de deux jours de réunion en vue de valider le planning et les modalités pratiques de cette phase ;
- met à disposition tous les éléments et documents produits par ou remis au présent titulaire ;
- présente l'ensemble des composants techniques ou fonctionnels du projet ; répond aux questions du futur titulaire concernant l'organisation pratique des configurations et des documents techniques sous 48 heures ;
- présente l'organisation de la maintenance corrective actuelle et l'environnement de développement et d'exploitation (répertoires, installation, procédures mises en oeuvre, périodicité et ordonnancement des opérations d'exploitation, etc.) ;
- accueille, durant deux semaines, deux ou trois personnes du futur titulaire afin de leur permettre d'observer l'activité assurée par l'équipe projet en place (assistance téléphonique, exploitation de serveurs de développement, etc.) ;
- communique au futur titulaire les réponses apportées aux demandes d'assistance téléphonique traitées.

3.11 - Résiliation

Les clauses de résiliations sont indiquées dans le CCAP TIC, se référer aux :

- Chapitre 5 article 37
- Chapitre 8 articles 47 à 54

4 - Exigences de sécurité

4.1 - Gestion de la sécurité

Le candidat précisera les moyens mis en œuvre dans le cadre du processus d'amélioration continu de la sécurité des infrastructures dont il a la charge.

Cette description peut être 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).

4.2 - Traitement des incidents de sécurité

- Remontée d'alerte : le service de supervision du titulaire met en place un système de remontée d'alerte visible de la DIR, 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 technique 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 désigné 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 la DIR, 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 la DIR ou un tiers désigné à participer au traitement de l'incident (si l'acheteur le souhaite).

4.3 - Exigences relatives aux achats de matériel

Lors de l'achat de matériel, plusieurs risques cyber doivent être pris en compte pour garantir un bon niveau de sécurité de la DIR. Voici les principaux risques à considérer décrits dans les paragraphes suivants.

4.3.1 - Vulnérabilités matérielles

Le titulaire doit s'assurer que le matériel proposé et fourni ne contient pas de vulnérabilités connues et exploitables par des cyberattaquants. Il devra vérifier que le matériel acheté est à jour avec les derniers correctifs de sécurité, qu'il respecte les niveaux d'exigences du présent CCTP et qu'il est compatible avec les systèmes de sécurité existants à la DIR.

En cas de remplacement des matériels obligatoire, suite à l'identification d'une faille permettant l'accès aux données pendant la durée du marché, le titulaire s'engage à proposer un matériel équivalent compatible avec le système mis en œuvre sous un délai de 5 jours ouvrés.

4.3.2 - Fournisseurs tiers

Les fournisseurs de matériel et de prestations de maintenance peuvent être des vecteurs de risques cyber. Le titulaire doit respecter les normes et bonnes pratiques de cybersécurité. La DIR se réserve le droit d'évaluer la sécurité du titulaire et des sous-traitants et s'assurera qu'ils respectent les normes et bonnes pratiques de cybersécurité.

4.3.3 - Logiciels embarqués

Le matériel peut inclure des logiciels embarqués qui présentent des risques de sécurité. Le titulaire doit vérifier que ces logiciels sont sécurisés et qu'ils peuvent être mis à jour régulièrement pour corriger les vulnérabilités éventuelles.

4.3.4 - Compatibilité avec les systèmes existants

Le nouveau matériel doit être compatible avec les systèmes de sécurité existants de la DIR. Une incompatibilité peut créer des failles de sécurité exploitables par des attaquants. La DIR pourra refuser un matériel proposé si son niveau de sécurité n'est pas suffisant ou incompatible avec les matériels et mesures déjà en place.

4.4 - Connaître le Système d'Information

4.4.1 - État de l'art Connaître le Système d'Information

Afin d'anticiper les obsolescences logicielles, il est demandé, lors du remplacement d'un système ou équipement existant ou lors de la rénovation de ce dernier, d'**établir un inventaire des systèmes, applications et matériels** qui seront déployés au sein du système d'information et des réseaux de la DIR.

Pour chacun des composants du système qui seront déployés, il est demandé :

- d'identifier le type de l'équipement,
- d'identifier la localisation dans l'équipement,
- de fournir la version applicative déployée, et celle préconisée par l'éditeur,
- de fournir la date de fin de support des logiciels si annoncée par l'éditeur ou le constructeur,
- d'indiquer la date d'application des derniers correctifs de sécurité,
- de lister les dépendances avec d'autres composants du SI.

Le titulaire fournit la preuve de conformité pour chaque nouveau matériel proposé.

4.4.2 - Cartographie des systèmes

Le titulaire dispose d'un inventaire et d'une cartographie des systèmes d'information dont il à la charge et doit les maintenir, selon les préconisations de l'ANSSI 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 à chaque mise à jour majeure du système.

4.5 - Gestion des identités et des accès

4.5.1 - 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**. Il est impératif de partir du principe que les configurations par défaut des systèmes d'information sont systématiquement connues des potentiels attaquants.

Les éléments d'authentification par défaut des composants du système installé doivent donc être modifiés dès leur installation et, s'agissant des mots de passe, ils devront être conformes à la politique de gestion des mots de passe suivante :

- Les mots de passe pour les profils utilisateurs doivent contenir 12 caractères ou plus, et être composés d'au moins un caractère de chacun des types suivants:
 - majuscules,
 - minuscules,
 - chiffres,
 - caractères spéciaux.
- Les mots de passe pour les profils administrateurs doivent contenir 16 caractères ou plus, et être composés d'au moins un caractère de chacun des types suivants:
 - majuscules,
 - minuscules,
 - chiffres,
 - caractères spéciaux.
- Les mots de passe ne doivent pas être vulnérables aux attaques par dictionnaire.

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

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.

Lorsque cela est nécessaire l'authentification à double facteurs sera mise en œuvre.

4.5.2 - Contrôle des authentifications

Afin de rendre plus difficiles les attaques sur les authentifications (attaque par brute force ou par dictionnaire), il est **imposé une augmentation du délai entre deux tentatives de connexions et ceci à partir de la 3^e tentative**.

Il est également demandé de vérifier que le stockage des mots de passe dans les configurations des équipements soit réalisé à l'aide d'un chiffrement conforme au Référentiel Général de Sécurité, **annexe B1 du [DR09]**.

4.5.3 - Inventorier les comptes utilisateurs et leur niveau de privilège

Des **comptes nominatifs** doivent être mis en place.

Il est demandé de lister les utilisateurs et leur rôle au sein du système qui sera déployé.

En complément, il est demandé de fournir la liste :

- des comptes de services (hiérarchisés),
- des comptes d'administration.

Le **principe du moindre privilège** est appliqué à tous les types de compte. Le principe du moindre privilège est le principe selon lequel chaque intervenant doit disposer d'un compte ayant exactement les droits nécessaires à l'accomplissement de ses tâches.

4.5.4 - Stockage sécurisé des mots de passe

Le stockage des mots de passe doit se faire dans un outil de coffre-fort numérique chiffré. La solution logicielle recommandée sur le parc de la DIR pour le stockage sécurisé des mots de passe sont les solutions :

- KeePass disponible sur Windows
- KeePassX pour les environnements sous Linux
- Bitwarden pour certains cas de coffres forts partagés.

4.6 - Gestion des flux

4.6.1 - Confidentialité et intégrité des flux

Tous les flux d'administration doivent être chiffrés par des procédés fiables (SSH, SSL, Ipsec, 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 oeuvre pour garantir la confidentialité et l'intégrité des flux d'administration.

Les protocoles réseaux suivants sont considérés comme non sécurisés et sont proscrits du réseau technique de la DIR :

- telnet,
- HTTP,
- IMAP,
- SMTP,
- POP3,
- FTP,
- rlogin,
- rcp,
- rsh,
- LDAP,
- VNC.

Bien qu'il soit difficile d'en dresser une liste exhaustive, les protocoles les plus courants

reposent sur l'utilisation de TLS [DR14] et sont souvent identifiables par l'ajout de la lettre « S » (pour secure en anglais) à l'acronyme du protocole.

4.6.2 - Contrôle et filtrage des flux

De manière générale, le filtrage des flux ne fait pas partie du périmètre du marché et est assuré par les équipes sécurité de la DIR.

Néanmoins, dans le cadre du déploiement d'une nouvelle infrastructure ou de l'évolution d'une infrastructure existante, le titulaire devra respecter les principes énoncés dans ce paragraphe.

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 à la DIR.

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. La fourniture de pare-feux ou tout autre équipements assurant le filtrage autre que les pare-feux des systèmes d'exploitation, ne fait pas partie du périmètre du marché. La solution proposée devra s'appuyer sur les matériels déjà existants à la DIR et devra tenir compte de l'infrastructure déjà en place.

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.

L'accès à distance pour la télémaintenance ne peut se faire que par la solution de télémaintenance mise à disposition du titulaire par les DIR ou par le Ministère.

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

4.6.3 - Protéger les expositions directes sur Internet

Dans les cas particuliers d'exposition d'un équipement ou d'un composant du SI sur Internet, il est demandé de se rapprocher de l'équipe réseau des DIR afin d'étudier la conformité. Un équipement raccordé au réseau des DIR ne doit en aucun cas être connecté à internet via une connexion externe de type partage de connexion 4G ou autre.

4.7 - Protection antivirale

La système, l'application ou le matériel livré par le titulaire devra supporter une protection antivirale fournie par la DIR.

Les restrictions liées à l'utilisation d'un antivirus devront être listées et argumentées par le titulaire.

4.8 - Gestion des mises à jour

4.8.1 - Mise à jour des correctifs de sécurité

Le titulaire informe les DIR dès la parution d'une alerte de sécurité portant sur un des composants du système couvert par le présent marché.

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 (Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques), le titulaire doit alerter les DIR dans un délai de 4 heures ouvrées maximum. Le correctif ou une solution palliative doit être appliqué dans un délai de 48 heures sur les infrastructures hébergeant le système du donneur d'ordres (serveurs, pare-feux, routeurs ouverts vers l'extérieur).

Lorsqu'aucun correctif n'est disponible, le titulaire doit suivre les recommandations de l'éditeur ou du CERT 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 et pourra se faire de manière groupée en une seule et unique mise à jour sur accord des DIR concernées.

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 préproduction.

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.

En cas d'alerte donnée par les équipes d'experts du titulaire, par l'administration ou le CERT, 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.

4.8.2 - Cas particulier d'utilisation de systèmes obsolètes

Si des **systèmes obsolètes** (qui ne sont plus supportés par leurs fabricants) devaient être déployés provisoirement, il conviendra de les **identifier** pour les **soumettre à validation de l'équipe cybersécurité des DIR afin de les isoler** au maximum du reste du SI des DIR.

Cette mesure s'applique aussi au niveau du réseau par un filtrage strict des flux, tout comme elle s'applique au niveau des secrets d'authentification qui doivent être dédiés à ces systèmes obsolètes.

4.9 - Sauvegarde et restauration

Le titulaire doit s'assurer que toutes les mesures qui s'imposent en termes de sauvegarde et de restauration pour se conformer au niveau de service exigé ont été mises en œuvre par les DIR. Les DIR gère indépendamment leurs sauvegardes, néanmoins le titulaire s'assurera de la bonne mise en œuvre des stratégies de sauvegarde (à minima se basant sur le principe 3-2-1-1-0) et apportera son conseil en cas de pratiques insuffisantes ou améliorables.

Lors de chaque visite préventive, le titulaire s'assurera qu'une sauvegarde valide est à disposition et qu'elle est conservée dans ses locaux pendant la durée du marché. Le titulaire doit s'assurer que des mesures permettant de garantir la confidentialité des

données relatives aux sauvegardes est effective :

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

Les sauvegardes externalisées doivent être chiffrées avant leur transfert et la clé de chiffrement connue seulement du titulaire et du donneur d'ordres.

La fiabilité des sauvegardes sera mise à l'épreuve par des tests de restauration bi-annuels ou à l'occasion des visites préventives, dont les rapports seront communiqués dans le mois suivant les tests.

4.10 - Continuité de l'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.

4.11 - Imputabilité et traçabilité

Les informations suivantes devront être enregistrées et stockées de manière sécurisée :

- 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.

4.12 - Durcissement des configurations

4.12.1 - Utilisation d'un système d'exploitation durci

Le prestataire utilisera, pour l'installation de son système ou de son application, **uniquement des systèmes d'exploitation durcis** selon les recommandations des guides CIS.

Pour chaque mesure non applicable, le titulaire fournira un motif motivé de dérogation à la mesure de durcissement et le cas échéant la mesure compensatoire mise en œuvre.

4.12.2 - Restriction des collectes de données

Il s'agit de **configurer les systèmes pour limiter les données recueillies par l'éditeur d'une solution dans le but de maîtriser la confidentialité de ses données.**

Il est demandé d'appliquer les mesures suivantes sur les systèmes d'exploitation Windows afin de restreindre les collectes de données et leur diffusion :

- Désactivation du service de télémétrie,
- Désactivation de l'agent Cortana,
- Restriction de l'utilisation de Windows Desktop Search à des recherches locales,
- Désactivation de l'envoi de rapports d'erreurs et de diagnostic,
- Désactivation de la personnalisation des saisies clavier, vocales et manuscrites,
- Désactivation du programme d'amélioration de l'expérience utilisateur,
- Désactivation de la géolocalisation,
- Désactivation de l'identifiant unique de publicité utilisé pour partager les informations collectées,
- Désinstallation des applications universelles non utilisées,
- Pas d'utilisation d'un compte Microsoft pour l'ouverture de session utilisateur,
- Désactivation du stockage dans le cloud One Drive.

4.12.3 - Restriction sur l'utilisation des supports amovibles

Il est demandé de **désactiver les exécutions automatiques** (autorun).

Il est demandé de **déclencher automatiquement un scan antivirus lors de l'insertion d'un média amovible.**

Sur les systèmes Linux, il est demandé de mettre en place la directive noexec sur les supports amovibles.

4.13 - Sécurisation des réseaux

4.13.1 - Réseaux Wifi

Il est demandé de suivre les recommandations [DR06] de l'ANSSI qui s'appliquent aux réseaux Wifi sur des périmètres industriels [DR07].

Il est demandé de **privilégier les installations filaires**, et sur obtention d'une dérogation de l'équipe cybersécurité, de respecter à minima l'ensemble des directives suivantes :

- Lorsqu'il s'agit de configurer un point d'accès Wifi, il est demandé de configurer le point d'accès pour utiliser un chiffrement robuste. Le mode WPA2 avec l'algorithme de chiffrement AES-CCMP est fortement recommandé,
- Il est demandé de s'interfacer avec une infrastructure d'authentification centralisée en s'appuyant sur WPA-Entreprise (standard 802.1x et protocole EAP), et d'utiliser une des

méthodes d'authentification suivantes :

- EAP-TLS, qui exige toutefois une Infrastructure de Gestion de Clés (IGC), avec clé privée et certificat à déployer auprès de chaque utilisateur. Lorsqu'EAP est utilisé, il convient par ailleurs que les clients vérifient l'authenticité du serveur d'authentification ;
 - EAP-TTLS, qui ne nécessite que le déploiement de certificats X509 serveurs et peut donc s'avérer plus pratique lorsqu'il est difficile de déployer des certificats clients. Ceux-ci s'authentifient alors généralement par couple utilisateur/mot de passe. Le support EAP-TTLS n'étant pas natif sous Windows, il convient de s'assurer qu'il est pris en charge par les clients Wi-Fi potentiels ;
 - PEAP, similaire à EAP-TTLS mais nativement pris en charge par Windows.
- Lorsque que le point d'accès Wi-Fi prend en charge la fonctionnalité de private Vlan invité et afin d'améliorer la protection en confidentialité des flux entre terminaux connectés à un même réseau Wi-Fi, il est demandé de le configurer en mode isolated.
 - Il est demandé de désactiver systématiquement la fonction WPS (Wi-Fi Protected Setup) des points d'accès.
 - Sécuriser l'administration du point d'accès Wi-Fi, en:
 - utilisant des protocoles d'administration sécurisés (par exemple, HTTPS),
 - connectant l'interface d'administration à un réseau filaire d'administration sécurisé, a minima en y empêchant l'accès aux utilisateurs Wi-Fi,
 - utilisant des mots de passe d'administration robustes (respectant la politique de gestion des mots de passe présentée au chapitre Changer les éléments d'authentification par défaut sur les équipements et services), d'une longueur supérieure à 20 caractères.
 - Il est demandé de remonter les événements de sécurité vers l'équipe réseau de la DIR.
 - Lorsque des données sensibles (au sens RGPD [DR15]), doivent être véhiculées via le réseau Wi-Fi, l'utilisation d'un protocole de sécurité spécifique, tel que TLS [DR14] ou IPsec, doit être mise en oeuvre.
 - N'activer l'interface Wi-Fi que lorsqu'elle celle-ci doit être utilisée.
 - Désactiver systématiquement l'association automatique aux points d'accès Wi- Fi configurés sur les terminaux.
 - Maintenir le système d'exploitation et les pilotes Wi-Fi des terminaux à jour des correctifs de sécurité.

4.13.2 - Création ou extension de réseaux

En cas d'ajout ou de modification d'équipements réseaux du parc des DIR il est nécessaire de respecter les préconisations suivantes :

Faire valider par l'équipe de maintenance des DIR :

- l'architecture réseau proposée,
- la compatibilité des équipements réseaux déployés avec le reste du parc d'équipements en production,

La configuration d'équipements réseaux déployés au sein du parc des DIR sera réalisée sous contrôle d'un technicien de la DIR concernée.

4.14 - Sécuriser l'administration

4.14.1 - Utiliser les protocoles d'administration sécurisés

Il est imposé de **n'utiliser que des protocoles d'administration sécurisés** [DR04] sur les systèmes et équipements, il est donc demandé en particulier :

- d'abandonner HTTP au profit de HTTPS, avec TLS en version TLS1.3 minimum,
- d'abandonner Telnet au profit de SSH, en version SSHv2 minimum.

4.15 - Sécuriser les applications web

Les mesures suivantes sont imposées pour **renforcer les protections d'un site web** [DR11] contre les attaques :

- Les architectures web de type « n-tiers » se prêtent bien à une approche de type défense en profondeur [DR18]. Il convient de ne pas concentrer toutes les mesures de sécurité sur le « tiers » présentation, mais au contraire de développer chaque composant afin qu'il assure sa propre protection.
 - Les droits sur les bases de données utilisées par les applications web doivent être gérés finement pour mettre en œuvre également le principe de moindre privilège.
 - La transformation des mots de passe doit faire intervenir un sel23 aléatoire.
- Les traitements doivent tous être faits du côté du serveur. Les entrées en provenance des clients ne doivent pas être considérées comme fiables et par conséquent, aucune vérification ne doit être déléguée aux clients.
 - Par exemple, si le code Javascript exécuté coté client peut faire certains contrôles à des fins d'ergonomie (pour signaler une probable faute de frappe dans un champ par exemple), il ne faut en aucun cas se contenter de ce contrôle. Il faut au contraire partir du postulat que le code client a pu ne pas s'exécuter (javascript désactivé ou requêtes malveillantes).

4.16 - Choix des composants du système

4.16.1 - Privilégier l'usage de produits qualifiés par l'ANSSI

La qualification est prononcée par l'ANSSI et permet d'attester d'un niveau de sécurité et de confiance dans les produits et les prestataires de service listés dans les catalogues que publie l'agence.

La qualification offre donc des garanties de sécurité et de confiance sur les produits ou les prestations de service.

Cette qualification fait suite à une étude approfondie du fonctionnement technique de la solution et de son écosystème. **Il est demandé de privilégier l'usage de produits qualifiés par l'ANSSI lorsqu'ils sont définis.**

A titre d'exemple, la solution de « coffre-fort » de mots de passe KeePass2 a obtenu, pour sa version 2.10 portable, une Certification de Sécurité de Premier Niveau (CSPN) par l'ANSSI.

4.17 - Journalisation

Il est imposé la journalisation [DR13] des accès aux données et des opérations effectuées suivants (horodatés et conservés pendant au moins un an) :

- pare-feu :
 - paquets bloqués,
- systèmes et applications :
 - authentification :
 - réussites et échecs d'authentifications,
 - gestion des comptes et des droits :
 - modification des données d'authentification (ajout ou suppression de compte / rôle et affectation de droits)
 - Modification des stratégies de sécurité :
 - édition / application / réinitialisation de configuration,
 - activité des systèmes et des processus :
 - démarrages / arrêts,
 - dysfonctionnements / surcharges du système,
 - chargements / déchargements de modules,
 - activité matérielle (défaillances, connexions / déconnexions physiques)
 - services :
 - erreurs de protocoles (par exemples les erreurs 403, 404 et 500 pour les services HTTP),
 - traçabilité des flux applicatifs aux interconnexions (URL sur un relai HTTP, en-têtes des messages sur un relai SMTP, etc.).
- antivirus :
 - détections d'éléments suspects par l'antivirus.

Afin de pouvoir corréler ces événements entre différents composants, leur source de

synchronisation de temps (grâce au protocole NTP) doit être identique.

4.18 - Contrôle de la prise en compte de ces mesures avant le déploiement en production

Il s'agit de **passer en revue la prise en compte par les projets de l'ensemble des mesures de cybersécurité listées** dans le présent document.

A cette fin, il est demandé d'envoyer à l'équipe cybersécurité de la DIR tous les éléments lui permettant d'apprécier la prise en compte des différentes mesures.

Si l'équipe cybersécurité de la DIR le juge nécessaire, des tests plus approfondis pourront être exigés avant la mise en production, par exemple via la mise à disposition d'une plateforme de tests ou de préproduction. À défaut, la vérification de l'application des mesures de sécurité pourra être vérifiée une fois le déploiement en production réalisé.

4.19 - Personnels en charge des prestations

4.19.1 - Liste de personnels intervenant sur le SI

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 de la DIR).

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.

4.19.2 - Qualification et formation dans le domaine de la SSI

Le titulaire sensibilise son personnel, intervenant dans le cadre des prestations, à la sécurité des systèmes d'information et aux règles de la DIR.

Le titulaire veille notamment à ce que sont personnel intervenant dans le cadre des

prestations respecte les dispositions concernant la sécurité du présent marché.

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 de l'hébergeur aux enjeux de sécurité.

4.19.3 - Exigences de sécurité pour les personnels extérieurs

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 de la DIR. Cette exigence peut être étendue à tous les types de soutiens (ménage, chauffage, climatisation, etc) si la sensibilité du système le justifie.

5 - Exigences de sécurité spécifiques pour les SI hébergés chez le titulaire

Ce chapitre ne concerne pas l'architecture actuelle mise en œuvre au sein des DIR. Néanmoins si l'architecture devait évoluer au cours du marché vers une solution hébergée nationale ou déportée, ce chapitre s'exercerait de plein droit.

5.1 - Sauvegarde 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.

5.2 - Continuité de l'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.

5.2.1 - Mise à jour des 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 (Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques), le correctif ou une solution palliative doit être appliqué dans un délai de 24 heures sur les infrastructures hébergeant le système du donneur d'ordres (serveurs, pare-feux, routeurs ouverts vers l'extérieur).

Lorsqu'aucun correctif n'est disponible, le titulaire doit suivre les recommandations de l'éditeur ou du CERT 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 préproduction.

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, 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.

5.3 - Protection des locaux

5.3.1 - 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.

5.3.2 - Protection contre les incendies

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.

5.3.3 - 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 la DIR : filtrage des accès au bâtiment ou aux étages, et filtrage des accès aux salles machines. Il définira les conditions d'accès de la DIR 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.).

5.3.4 - 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 des DIR. 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.

6 - Bonnes pratiques pour l'hébergement mutualisé

Ce chapitre ne concerne pas l'architecture actuelle mise en œuvre au sein des DIR. Néanmoins si l'architecture devait évoluer au cours du marché vers une solution hébergée nationale ou déportée, ce chapitre s'exercerait de plein droit.

6.1 - Journaux d'événements et conservation des traces

Le prestataire est tenu de s'assurer qu'une journalisation des accès et des événements (système, Web...) est activée sur tous les équipements dont il a la charge. Une politique de sauvegarde de ces traces doit exister (deux mois de sauvegarde sont demandés sur les pare-feux et les serveurs Web).

Le donneur d'ordres peut être amené à demander un extrait de ces traces, soit dans le cas d'un incident, soit à des fins de suivi de la (des) ressource(s).

Conditions d'accès à ces journaux :

- la DIR doit pouvoir avoir accès aux journaux d'événements (réduits éventuellement à un extrait) à sa demande et dans les délais contractualisés (ex. : dans la journée). L'idéal est que la DIR ait un moyen de suivi des événements en temps réel ;
- la DIR doit, de plus, être sûr que les journaux concernant ses ressources hébergées ne sont pas divulgués à d'autres organismes co-hébergés (garantie de confidentialité) ;
- l'hébergeur doit certifier que toutes les informations présentes sur les journaux sont exploitables au regard de l'état de l'art (pas de biais horaire ou biais horaire maîtrisé et documenté, journaux déportés ou copiés sur une autre machine, etc.).

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

6.2 - Suivi du service hébergé

Outre le contrôle des journaux d'événements, il est nécessaire de pouvoir disposer d'indicateurs sur l'historique du service hébergé. Il est ainsi possible de dégager les principaux événements relatifs à l'utilisation du service, ce qui permet d'avoir accès à des événements ayant précédé une éventuelle crise. Les indicateurs les plus courants sont (liste non exhaustive) :

- fréquence et suivi des mises à jour effectuées (indispensable) ;
- durée d'indisponibilité maximum et suivi de ces indisponibilités ;
- fréquence des sauvegardes et tests de restauration effectués ;
- indicateurs sur les ressources dont l'accès et la mise à disposition ne dégradent pas la sécurité du système d'information :
 - charge réseau pour le serveur et pour la ressource ;
 - charge processeur utilisée par la ressource et pourcentage de la charge du serveur ;
 - charge mémoire utilisée par la ressource et pourcentage de la charge du

- serveur ;
- etc.

De la même manière, il est nécessaire que les DIR connaissent au préalable l'origine et/ou la teneur des services co-hébergés, ce qui permettra d'étayer leur analyse de risques.

Dans le meilleur des cas, il conviendra d'opter pour une solution hybride de cohébergement.

Celle-ci consiste à n'héberger sur un serveur donné qu'un ensemble de ressources, appartenant toutes à la même organisation, ou fruit d'une communauté d'intérêt. Il sera alors plus facile d'obtenir un accord écrit de la communauté sur l'accès à la machine pour analyse en cas d'incident.

6.3 - Prévention d'une attaque

Le contrat passé avec l'hébergeur doit prévoir le cas d'éventuelles attaques informatiques. La réactivité en cas d'incident étant extrêmement importante, il conviendra de faire figurer dans le contrat les points suivants :

- identification d'un contact technique (ou plusieurs) clairement identifié chez l'hébergeur ainsi que pour la DIR, joignable 24/24, 7/7, tous les jours de l'année ;
- identification d'un contact décisionnel (ou plusieurs) clairement identifié chez l'hébergeur ainsi que pour la DIR, joignable 24/24, 7/7, tous les jours de l'année ;
- garantie d'information immédiate : la DIR doit être tenue informée sans délai en cas d'attaque afin de déclencher le circuit de réaction adéquat ;
- définition des procédures de remontée d'incident ;
- définition claire et exhaustive avec l'hébergeur de ce que l'on entend par incident (défiguration, temps d'indisponibilité, etc.).

6.4 - Réaction sur incident

En cas d'incident, seule la DIR doit avoir le contrôle total sur la marche à suivre. Ainsi, le contrat doit prévoir que :

- la désignation de l'organisme chargé de traiter l'incident doit être laissée à la seule appréciation de la DIR ;
- cet organisme doit pouvoir jouir au nom de la DIR d'un contrôle total de l'environnement de la ressource à des fins d'analyse. Par exemple :
 - prélèvement de tout élément nécessaire à l'analyse conformément aux règles de l'art ;
 - analyse du système en fonctionnement.
- la gestion de l'incident et de la conduite des actions postérieures sont à la seule initiative de la DIR. Ceci comprend :
 - toute action sur la machine : redémarrage, arrêt, rétablissement d'une sauvegarde, isolement physique du reste du réseau,
 - établissement d'un périmètre de sécurité, etc. ;
 - délai d'indisponibilité de la ressource ;

- délai d'indisponibilité du serveur et pénalités d'astreinte éventuelles ;
contrôle sur les règles de filtrage.

7 - ANNEXE 1 : Exemple de clauses de confidentialité type en cas de sous-traitance

Les supports informatiques et documents fournis par la société [identité du responsable de traitement] à la société [identité du prestataire] restent la propriété de la société [identité du responsable de traitement].

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 la société [identité du responsable de traitement].

La société [identité du responsable de traitement] 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].