

CAHIER DES CLAUSES TECHNIQUES PARTICULIERES (CCTP)

Solution externalisée de supervision et de
management des infrastructures réseaux (Lan et
Wifi)

Réf. : CCIR-DSI-2026-21

SOMMAIRE

1	OBJET du marche	3
2	LE PERIMETRE TECHNIQUE.....	3
2.1	La console de gestion ATTENDUE	4
2.2	LE PORTAIL CAPTIF	5
2.3	LES PRESTATIONS WIFI COMPLÉMENTAIRES.....	6
2.4	LE contrôle D'ACCES RESEAU SECURISÉ.....	7
3	PRESTATIONS ASSUREES PAR LE TITULAIRE	7
3.1	LA MAINTENANCE PREVENTIVE	7
3.2	LA MAINTENANCE CORRECTIVE.....	8
3.3	COMITÉS DE PILOTAGE	9
4	OBLIGATIONS DU TITULAIRE	9
5	INTERVENTIONS DU TITULAIRE SUR LES INSTALLATIONS	10
6	EXIGENCES DE SECURITE	11
6.1	Mises à jour, correctifs de sécurité	11
6.2	Continuité d'activité.....	12
6.3	Protection antivirale.....	12
6.4	Sauvegardes et restauration	13
6.5	Authentification	13
6.6	Confidentialité et intégrité des flux	14
6.7	Contrôle et filtrage des flux.....	14
6.8	Imputabilité, traçabilité.....	14
6.9	Personnels en charge des prestations	15
6.10	Qualifications et expérience, formations et sensibilisation dans le domaine de la SSI des personnels en charge des prestations.....	15
6.11	CONTINUITE DES SERVICES ESSENTIELS : ENERGIE, CLIMATISATION ET TELECOMMUNICATIONS 15	
6.12	PROTECTION CONTRE LES INCENDIES, LA FOUDRE ET LES DEGATS DES EAUX	16
6.13	Surveillance et contrôle des accès aux locaux de l'hébergeur, en particulier au local d'hébergement du système d'information	16
6.14	Intervention DE maintenance ou de support	16
6.15	AuditS de sécurité	17
6.16	Protection des données	17
6.17	REVERSIBILITE.....	18

1 OBJET DU MARCHÉ

La CCI de région Hauts de France s'appuie sur une plateforme cloud hautement disponible pour gérer et superviser ses infrastructures Wifi et Lan, ainsi que gérer les usagers des réseaux Wifi par l'intermédiaire d'un portail captif associé.

Les switchs et bornes wifi à gérer sont de marque Aruba et aucun changement n'est envisagé dans le cadre de ce marché.

L'intégralité des actions à mener pour réintégrer sur la plateforme les éléments d'infrastructure Aruba Lan et Wifi seront à la charge du titulaire. Parmi ces actions nous retrouverons entre autres la reprise des chartes d'utilisation, des spécificités de chaque site, et la configuration du NAC et du relai local en limitant les interruptions de service, si nécessaire la réinitialisation des bornes Wifi, la cartographie.

En prévision de nouveaux projets, susceptibles d'être interfacés avec ces solutions (par exemple utilisation d'une plateforme web de gestion d'espaces de Coworking), les plateformes devront permettre l'utilisation d'API (interface de programmation d'application). Elles devront également être interfaçables avec plusieurs annuaires en fonction des portails (Idaps, plusieurs Active directory...), permettre l'interrogation de bases de données (clients, coworkers) et de webservices. D'autres modes de connexion sur les hotspots wifi visiteurs peuvent être abordés (Linkedin...). Il est demandé aux candidats de détailler ces points.

Pour des raisons de sécurité les paramétrages détaillés des sites en production seront communiqués uniquement au titulaire, le périmètre global et les fonctionnalités attendues sont décrites dans ce CCTP.

L'hébergement des plateformes proposées devra être exclusivement localisé en France.

L'obligation d'héberger les données sur des serveurs situés en France vise à garantir leur sécurité, leur confidentialité et leur disponibilité, ainsi qu'une application pleine du droit français et européen, notamment en matière de protection des données. Cette exigence permet de limiter les risques liés à des législations extraterritoriales et de renforcer le contrôle de l'acheteur public sur les conditions d'hébergement. Elle est justifiée par la nature sensible des données confiées par l'acheteur et les exigences de continuité et de fiabilité du service, et demeure strictement limitée à l'objet du marché.

2 LE PERIMETRE TECHNIQUE

Le périmètre traité par la consultation concerne l'ensemble des sites CCI Hauts de France, et centres de formation LAHO Formation, répartis sur la région Hauts de France.

L'infrastructure intégrée à la plateforme sera amenée à évoluer en nombre de sites et d'équipements, cela représente à ce jour :

- **50 sites**
- **270 switchs Aruba**
 - 3810M, 16 ports.
 - 2930M, 48 et 24 ports.
 - 2930F, 48,24 et ports.
- **470 bornes Wifi Aruba**
 - AP207
 - AP303
 - AP305
 - AP334
 - AP335

- AP515
- AP535
- AP555
- AP565
- **Une solution d'écoute assistée**
 - MobileConnect de SENNHEISER (« Annexe-MobileConnect.pdf » en annexe)
- **7 portails captifs**
 - Détermination du portail captif en fonction du SSID.
 - Personnalisation par portail (charte graphique, charte d'utilisation, 1 Charte graphique, lien de connexion...).
 - Multi vlan.
 - Multi SSID.
 - Gestion par Zone.
 - Groupes de borne de modèles hétérogènes, ou SSID différents.
 - Un même portail captif peut être partagé sur plusieurs sites.
- En prévision de l'intégration progressive des switchs Aruba CX6000, les candidats devront préciser dans leur offre la manière dont ils comptent gérer la phase transitoire durant laquelle coexisteront nos équipements actuels (3810M, 2930M et 2930F) et les nouveaux matériels. Ils indiqueront également au bordereau des prix unitaires (BPU) les coûts associés à cette période transitoire en prenant en considération 2 modes de gestion des switchs (supervision ou management).

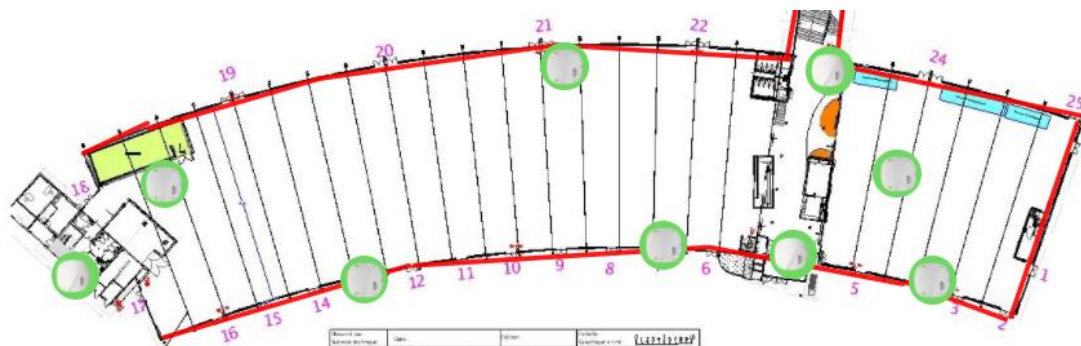
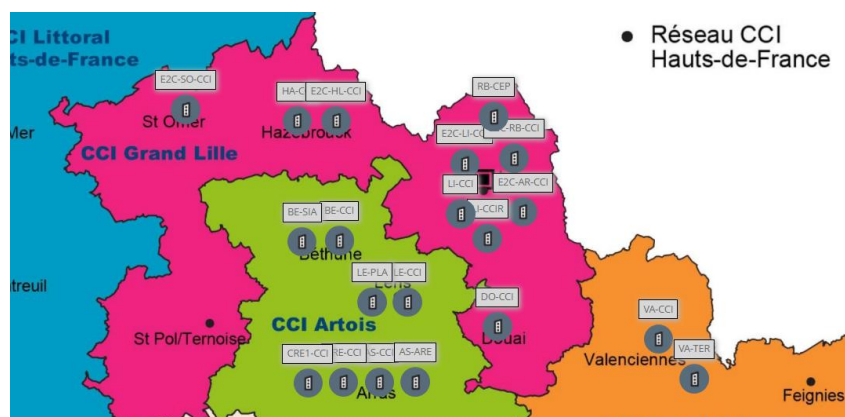
2.1 LA CONSOLE DE GESTION ATTENDUE

Les candidats présenteront en détail la console de gestion de la solution externalisée proposée.

La solution doit intégrer certains modules, parmi lesquels :

- **Supervision et management**
 - La supervision de l'architecture Wifi & Lan.
 - La supervision des utilisateurs Wifi & Lan.
 - La configuration centralisée des bornes Wifi (points d'accès), des contrôleurs et des switchs.
 - La supervision et le statut des services liés aux Wifi.
 - DNS.
 - DHCP.
 - Roaming.
 - Authentification.
- **Reporting et d'alerte**
 - Rapport d'état de fonctionnement, d'utilisation, etc.
 - Alerte en cas de panne, de problème (défaut d'un client, etc.)
- **Module de diagnostic de l'infrastructure et des clients**
 - Analyse de la chaîne de connexion des clients.
 - État de la radio (qualité, puissance, erreurs de transmission, etc.)
- **Module de localisation et cartographie**

- Cartographie de la couverture Wifi des sites.
- Détection des trous de couverture / interférences / point d'accès pirate / etc.
- Localisation des équipements Wifi.
- Module de simulation d'ajout ou perte de point d'accès.



2.2 LE PORTAIL CAPTIF

La CCI Hauts de France diffuse des réseaux de type hotspot à travers son infrastructure Wifi. Les flux de ces réseaux sont placés dans des VLAN dédiés.

Les candidats devront proposer un portail captif externalisé « clé en main », qu'ils devront gérer. L'intégralité des paramètres en exploitation devront être repris (charte graphique, charte d'utilisation du Wifi, bandes passantes autorisées, SSID, etc...).

L'échéance du contrat qui porte sur le portail captif en exploitation étant au 20 septembre 2026, le titulaire s'engage à intégrer l'ensemble des sites au nouveau portail au plus tard pour cette date, avec les reprises des paramètres actuels, et ce en dérogation de l'article 38.3 du CCAG TIC.

La solution proposée devra :

- Être personnalisable.
- Proposer différentes méthodes d'enregistrement.
 - Auto-enregistrement avec obligation d'accepter une charte (une charte type devra être proposée).
 - Par délégation : création du compte via une interface dédiée, simple d'utilisation.
 - Par parrainage : validation du compte invité par l'utilisateur de la CCI qui le reçoit.
 - Par import de masse (fichier Excel).
- Gérer les aspects légaux.

- Loi Hadopi, RGPD.
- Traçabilité des logs, déclaration CNIL.
- S'appuyer sur un certificat de confiance (fournit par le titulaire qui reprendra le même type de certificat et autorité de certification – Des postes non administrés par la CCI Hauts de France sont amenés à se connecter au réseau).
- Permettre la création d'une empreinte : lors de la première authentification d'un matériel, afin que celle-ci soit automatiquement reconnue et connectée (sans repasser par le portail captif) durant toute sa durée de validité.
- Permettre de définir les périodes de validité des comptes (durée, date de fin, volume de données, etc.)
- Permettre de limiter l'accès à certains protocoles.

Ce portail captif devra pouvoir supporter **au minimum 2000 sessions simultanées**.

2.3 LES PRESTATIONS WIFI COMPLÉMENTAIRES

Parmi ces prestations :

- Etude de couverture sur site.
- Etude de couverture sur plan.
- Mise en service d'un nouveau site (nouvelle agence, nouveau centre de formation...).
 - Sur ce point, la tarification renseignée intégrera l'ensemble des tâches nécessaires.
 - Mise en place d'un nouvel SSID.
 - Ajustement des débits sur un SSID.
 - Intégration d'une charte graphique spécifique.

La solution du titulaire doit permettre :

- La gestion des paramétrages spécifiques et sécurisés pour des objets connectés (IOT) de plus en plus indispensables et nombreux.
- La couverture voix pour les services de téléphonie mobile est parfois insuffisante dans nos locaux. Il pourrait être envisagé d'utiliser des solutions de voix sur Wifi à travers des différents SSID.
- La possibilité d'une interface avec des solutions de MDM (gestion des appareils mobiles), et avec quelles solutions.
- La possibilité d'une authentification via un annuaire Office 365.
- La possibilité de créer un portail de délégation convivial qui permettrait :
 - La création de SSID « à la volée » avec éventuellement l'interfaçage avec une application métier de gestion des réservations / Coworking.
 - De gérer la durée de vie SSID.
 - Exemple : Formation entreprise spécifique, pour une durée donnée, dans une salle définie, avec des attributions spécifiques de ports autorisés, de débit
- L'utilisation des hotspots Wifi pour des usages de coworking nécessiterait un autre mode de fonctionnement plus « ouvert » permettant aux coworkers une utilisation moins contrainte de leurs outils (sans blocage de ports). Il resterait cependant nécessaire de garantir la sécurité des équipements des utilisateurs de ce service vis-à-vis des autres coworkers (par exemple « private vlan » ...).

2.4 LE CONTROLE D'ACCES RESEAU SECURISÉ

Dans le but d'augmenter le niveau de sécurité de son infrastructure réseau, la CCI de région Hauts de France a automatisé en partie les politiques de sécurité appliquées aux équipements connectés sur ses réseaux, et cela quel que soit le mode de connexion (filaire ou sans fils).

Ce besoin répond à la constante augmentation du périmètre géographique et fonctionnel imposée aux équipes informatiques de la CCI HAUTS DE France, ainsi qu'aux nouveaux usages (connexions d'ordinateurs externes, smartphones, tablettes, objets IoT, adaptabilité des espaces pour des usages internes ou externes à la CCI, coworking...).

La CCI exploite le solution NAC Aruba ClearPass sur une partie de ses réseaux, et souhaite poursuivre le déploiement à plus grande échelle. Dans cette optique le niveau de licence actuel sera maintenu à 5000 Endpoints, et il est demandé aux candidats de préciser le coût d'un accompagnement de 15 jours par an sur cette technologie dans le bordereau des prix unitaires (BPU)

3 PRESTATIONS ASSUREES PAR LE TITULAIRE

Afin de garantir la bonne exécution du marché, la CCI et le titulaire conviendront d'une réunion de cadrage qui aura lieu dans les 15 jours après la notification du marché, afin de déterminer les rôles et responsabilités des intervenants. Cette réunion est réputée incluse dans l'offre de prix du titulaire.

Pour permettre l'exécution des clauses du marché, la CCI Hauts de France s'engage à laisser visiter les installations par les agents du titulaire.

Les heures ouvrées des établissements de la CCI Hauts-de-France sont réputées être de 8h à 19h.

L'offre du titulaire comporte a minima :

- La mise à jour des points d'accès en heures non ouvrées à la demande de la CCI ou en concertation avec les équipes de la CCI quand le titulaire le juge nécessaire.
- Une maintenance proactive et curative.
- **Une hotline illimitée** (par courrier électronique, téléphone, extranet ou alerte automatique de la supervision) en heures et jours ouvrés sur l'infrastructure Wifi et Lan.
- **La modification des configurations de manière illimitée.**
- L'envoi d'un rapport mensuel d'utilisation personnalisé.
- La rédaction d'un DAT pour l'ensemble des solutions déployées (documents de spécifications techniques).
- Un transfert de compétences sur toutes les solutions déployées.

L'intégration initiale des équipements sur la plateforme devra être étudiée pour limiter au maximum les interruptions de service. **Le titulaire veillera à réaliser les opérations impactantes en heures non ouvrées**, et fera valider au préalable le planning d'intervention par les équipes de la CCI Hauts de France.

Le titulaire prend exclusivement à sa charge toutes les interventions nécessaires à l'intégration des équipements sur la plateforme.

3.1 LA MAINTENANCE PREVENTIVE

La maintenance préventive comprend toutes les interventions et les actions nécessaires au suivi et au bon fonctionnement des systèmes ainsi que toutes les actions à mener par le titulaire, concourant à maintenir le niveau de qualité des systèmes à fonctionnalités identiques (fiabilité, robustesse, maintenabilité).

Sont également intégrées dans la maintenance préventive, **en heures non ouvrables**, la mise à jour des bornes Wifi, et l'intégration des correctifs de sécurité qui pourront faire suite à une annonce du CERT, du fabricant Aruba, ou simplement à la demande des équipes de la CCI Hauts de France.

Le titulaire du marché s'engagera à réaliser une maintenance préventive tel qu'il l'a détaillé dans son offre. La CCI de région Hauts de France attend notamment :

- Un rapport régulier des actions menées.
- Un suivi particulier des certificats de sécurité employés.

3.2 LA MAINTENANCE CORRECTIVE

La maintenance corrective comprend toute action à la suite d'une notification d'incidents, d'anomalies, permettant la résolution de l'incident, de l'anomalie et rendant de nouveau possible l'utilisation normale des systèmes. Il est rappelé que l'intervention de maintenance corrective est déclenchée exclusivement sur demande par tout moyen mis à disposition du service bénéficiaire (par courrier électronique, téléphone, extranet ou alerte automatique de la supervision).

Les opérations de maintenance corrective peuvent être consécutives :

- A une maintenance préventive.
- A un appel sur incident.
- A une information du constructeur (Aruba).

Toute opération de maintenance corrective se déroule sans interruption jusqu'à résolution complète de l'incident et retour au service opérationnel de l'ensemble. Conformément à l'article 14.2.4 du CCAG TIC, l'indisponibilité s'achève par la remise à disposition de l'acheteur des éléments, en état de marche. Toutefois, lorsque les éléments réparés sont à nouveau indisponibles, pour les mêmes causes, dans les huit heures d'utilisation après leur remise en état, la durée d'indisponibilité est décomptée à partir de la constatation de l'indisponibilité initiale.

Il existe deux niveaux de pannes, à savoir :

- Le niveau majeur (pannes bloquantes).
- Le niveau mineur (pannes non bloquantes ou qui génèrent un fonctionnement dégradé)

Pannes bloquantes

Entrent notamment dans cette catégorie :

- Indisponibilité supérieure ou égale à 50 % des ponts d'accès d'un site.
- Indisponibilité d'un SSID sur un site.
- Le Wifi devra être exploitable par tous types d'équipements, ordinateurs, tablettes, smartphones, tous types de systèmes d'exploitation confondus. L'impossibilité d'utiliser un réseau Wifi pour un type d'équipement sera considéré comme panne bloquante.

Durée maximale de l'indisponibilité

Par dérogation à l'article 14.2.3 du CCAG TIC, les délais maximums d'indisponibilité sont les suivants :

Maintenance corrective	Durée maximale d'indisponibilité avec déclenchement pendant heures ouvrables	Durée maximale d'indisponibilité avec déclenchement pendant heures non ouvrables
Panne bloquante	4 heures	12 heures
Panne non bloquante	8 heures	24 heures

Le non-respect de ces délais entraîne l'application des pénalités définies au CCAP.

3.3 COMITÉS DE PILOTAGE

Pour veiller à ce que soit assurée la qualité des services et des prestations, **un comité de pilotage trimestriel sera organisé par le titulaire durant toute la durée du marché**, avec la présence de l'interlocuteur dédié que le titulaire a indiqué dans son offre.

Cette réunion portera entre autres sur :

- Les rapports d'usage Wifi.
- Les incidents rencontrés.
- La synthèse des maintenances réalisées.
- L'identification et la mise en œuvre des améliorations (densité Wifi, services, sécurité ...)
- La planification des mises à jour.

4 OBLIGATIONS DU TITULAIRE

Il est indiqué que le titulaire doit :

- Lors de ses interventions sur les sites de la CCI, respecter le règlement intérieur.
- Assurer les prestations contractuelles sous sa responsabilité exclusive dans les conditions optimales de sécurité, de confort et d'économie.
- Assurer en cas d'urgence l'intervention dans les meilleurs délais.
- Soumettre au service bénéficiaire les solutions possibles visant à améliorer la fiabilité des installations ou à faire des économies.

- Désigner les responsables pouvant représenter le titulaire dans diverses circonstances.
- Se conformer à toutes les obligations définies par la législation, les normes et règles de l'art.
- Informer le service bénéficiaire des incompatibilités éventuelles des installations avec les règlements présents ou avec les objectifs fixés et lui proposer les dispositions à prendre.
- Rappeler dans les délais la nécessité de contrôles et mises en conformité et prêter aide et assistance aux Organismes de Contrôles Spécialisés.
- Assurer sous sa responsabilité l'organisation du travail, la discipline, le respect des consignes et l'efficacité du personnel dont il est responsable.
- N'apporter aucune modification aux installations sans l'accord de la CCI HAUTS-DE-FRANCE
- N'apporter aucune modification du mot de passe de l'installation sans en aviser le service bénéficiaire, celui-ci en est propriétaire.
- Restituer en fin de marché l'ensemble des documents d'exploitation réalisés.
- Se soumettre aux contrôles du service bénéficiaire. Ces contrôles éventuels sont effectués en présence d'un responsable du titulaire qui garde dans ce cas la responsabilité de ses propres manœuvres.
- Avertir le service bénéficiaire des mises en arrêt d'équipements nécessitées par l'entretien et convenir avec ce service, dans le cas où elles sont prévisibles, des dates d'arrêt par un échange écrit à l'initiative du titulaire.
- Justifier, à tout moment, et à compter de la signature du présent marché, qu'il a contracté les assurances habituellement nécessaires à l'exercice de sa profession.
- Tenir à jour les divers documents constatant la réalisation des tâches.
- Prendre toutes dispositions pour que le fonctionnement des installations ne soit pas perturbé.
- Faire au service bénéficiaire des propositions d'optimisation et d'améliorations. Ces propositions devront être chiffrées et argumentées avec investissement, temps de retour sur investissement, avantages et inconvénients.

5 INTERVENTIONS DU TITULAIRE SUR LES INSTALLATIONS

Dans le cadre de la maintenance réalisés sur les infrastructures Wi-Fi et LAN (installation, remplacement, déplacement ou modification d'équipements et de câblages), le titulaire s'engage à mettre en œuvre toutes les mesures nécessaires afin de préserver la sécurité, l'intégrité et la continuité du réseau existant.

À ce titre, le titulaire s'engage notamment à :

Préparation et encadrement des travaux

- Réaliser les travaux selon un mode opératoire définissant les impacts potentiels sur le réseau et les mesures de sécurisation associées ;
- Faire réaliser les travaux par du personnel disposant des habilitations électriques requises (NF C 18-510), de compétences techniques avérées en réseaux LAN et Wi-Fi, et dûment autorisé à intervenir en site occupé et dans les locaux techniques. Le titulaire garantit que ses intervenants sont formés aux règles de sécurité et aptes à intervenir sans porter atteinte à l'intégrité ni à la sécurité du réseau ;
- Faire valider préalablement par l'acheteur toute intervention susceptible d'entraîner une coupure, une modification de topologie ou de configuration réseau ;
- Planifier les interventions de manière à limiter les risques d'interruption de service.

Sécurisation physique des installations

- Assurer la protection des équipements, câbles, baies et locaux techniques pendant toute la durée des travaux ;
- Interdire tout accès aux infrastructures réseau à des personnes non autorisées ;
- Veiller à la conformité et à la sécurisation des raccordements réalisés (étiquetage, cheminements, fixation, fermeture des baies).

Maîtrise des modifications techniques

- Effectuer les travaux sans altérer les mécanismes de sécurité existants (segmentation réseau, configurations de sécurité, contrôles d'accès) ;
- Documenter toute modification apportée aux infrastructures ou à la configuration réseau ;
- Ne connecter au réseau que des équipements conformes aux exigences techniques et de sécurité définies par l'acheteur.

Remise en état et vérifications

- Procéder, à l'issue des travaux, à une remise en état complète des installations et des locaux techniques ;
- Réaliser des tests de bon fonctionnement du réseau concerné ;
- Signaler sans délai à l'acheteur tout incident, anomalie ou vulnérabilité constatée à l'occasion des travaux.
- Tout manquement aux obligations de sécurité lors des travaux pourra engager la responsabilité du titulaire.

Le cas échéant, les parties arrêteront un plan de prévention, conformément à l'article R4512-7 et suivants du Code du Travail.

6 EXIGENCES DE SECURITE

L'offre du titulaire tiendra compte des moyens à mettre en œuvre dans le cadre du processus d'amélioration continue de la sécurité des applications développées.

Cette description peut être à présenter selon les étapes :

- 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 à la suite des insuffisances constatées lors de la vérification).

6.1 MISES A JOUR, CORRECTIFS DE SECURITE

Le titulaire applique les correctifs recommandés par les fournisseurs de solutions matérielles ou logicielles (logiciels système ou applicatifs, logiciels embarqués) sur l'ensemble des solutions 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 doit être appliqué dans un délai de 24 heures sur les sites du donneur d'ordres (serveurs web, base de données, ...)

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 des applications et des données qu'il contient, ainsi que de tests sur un environnement de pré production.

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

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

En cas d'alerte donnée par les équipes d'experts du titulaire, par l'administration ou le CERT, 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 (heures ouvrables) permettant au maître d'ouvrage de suivre le traitement d'une alerte.

6.2 CONTINUITE D'ACTIVITE

Le titulaire doit prendre toutes les mesures nécessaires pour assurer la disponibilité de l'application, 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 de l'application, ou en cas de sinistre la reprise d'activité.

Les procédures de sauvegarde et de secours seront auditées conformément aux modalités identifiées dans la clause relative aux audits de sécurité du Plan d'Assurance Sécurité.

6.3 PROTECTION ANTIVIRALE

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

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

Le candidat fournira dans sa réponse une description des solutions anti-virus sur lesquelles se basent les serveurs et postes clients et décrira les modalités et la fréquence de mise à jour du service.

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

6.4 SAUVEGARDES ET RESTAURATION

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

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

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

Un double exemplaire des sauvegardes doit être conservé dans des locaux physiquement séparés du centre informatique du prestataire hébergeant l'application la CCI de Région Hauts de France.

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 la CCI de Région Hauts de France.

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

6.5 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 doivent impérativement authentifier un utilisateur.

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

- L'utilisation de mots de passe constructeur ou par défaut est interdite.
- L'utilisation de protocoles dont l'authentification est en clair est interdite.
- Les mots de passe doivent satisfaire aux contraintes de complexité suivantes :
 - Avoir une longueur minimale de 10 caractères (sauf limitation technique).
 - Comporter au minimum une majuscule, un chiffre et un caractère spécial.
 - Ne pas être vulnérables aux attaques par dictionnaire.

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

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

6.7 CONTROLE ET FILTRAGE DES FLUX

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 candidat.

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 notamment :

- Attaque en déni de service.
- Injection de code.
- Attaque par rebond.

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

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

6.8 IMPUTABILITE, TRAÇABILITE

Les informations suivantes devront être enregistrées :

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

6.9 PERSONNELS EN CHARGE DES PRESTATIONS

Le titulaire s'engage à informer la CCI sans délai de tout changement des personnels autorisés à intervenir sur les applications mises en place pour la CCI de Région Hauts de France, ainsi que leur niveau d'habilitation (types d'accès et ressources concernée).

6.10 QUALIFICATIONS ET EXPERIENCE, FORMATIONS ET SENSIBILISATION DANS LE DOMAINE DE LA SSI DES PERSONNELS EN CHARGE DES PRESTATIONS

Les moyens humains en charge des prestations du marché devront disposer des habilitations suivantes :

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

6.11 CONTINUITE DES SERVICES ESSENTIELS : ENERGIE, CLIMATISATION ET TELECOMMUNICATIONS

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.

6.12 PROTECTION CONTRE LES INCENDIES, LA FOUDRE ET LES DEGATS DES EAUX

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

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

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

6.13 SURVEILLANCE ET CONTROLE DES ACCES AUX LOCAUX DE L'HEBERGEUR, EN PARTICULIER AU LOCAL D'HEBERGEMENT DU SYSTEME D'INFORMATION

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

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

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.).

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

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 les applications mises en place pour la CCI de Région Hauts de France.

6.14 INTERVENTION DE MAINTENANCE OU DE SUPPORT

Les intervenants 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).

6.15 AUDITS DE SECURITE

La CCI HAUTS-DE-FRANCE pourra, à tout moment, contrôler que les exigences de sécurité sont satisfaites par les dispositions prises par le candidat.

Les audits pourront être réalisés par la CCI HAUTS-DE-FRANCE, ou faire appel à l'expertise d'un organisme ou d'une société tierce présentant des compétences en matière de sécurité.

Des analyses de vulnérabilité, des tests d'intrusion réseau ou applicatifs pourront être menés.

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 est à la charge du candidat.

6.16 PROTECTION DES DONNEES

Le titulaire s'engage à respecter l'ensemble des dispositions légales et réglementaires applicables en matière de protection des données à caractère personnel, notamment le Règlement (UE) 2016/679 du 27 avril 2016 (RGPD) et la loi n°78-17 du 6 janvier 1978 modifiée, dite « Informatique et Libertés ».

Les modalités détaillées relatives :

- aux rôles et responsabilités de chaque partie
- aux finalités et à la nature des traitements confiés ;
- aux catégories de données et de personnes concernées ;
- aux obligations du sous-traitant en matière de confidentialité, de sécurité organisationnelle et technique, et d'assistance ;
- aux conditions de recours à la sous-traitance ultérieure et de transfert de données hors UE ;
- aux modalités de notification des violations de données ;
- Ainsi qu'aux mesures de restitution, ou de suppression des données à l'issue du marché.

sont définies à l'article 13 du CCAP et dans ses annexes RGPD (Annexe 1 et 2) et Sécurité (Annexe 3).

Ces annexes doivent être complétées par le titulaire avant la notification du marché, conformément aux indications figurant dans le CCAP.

Le titulaire reconnaît avoir pris connaissance :

- de l'ensemble des exigences énoncées dans le CCAP et ses annexes RGPD et Sécurité ;
- des obligations lui incombant au titre du RGPD et de la réglementation applicable ;

et s'engage à les respecter intégralement pendant toute la durée d'exécution du marché.

6.17 REVERSIBILITE

Le titulaire s'engage à coopérer pleinement avec le pouvoir adjudicateur et, le cas échéant, avec tout nouveau prestataire désigné, pour assurer une transition maîtrisée, progressive et sécurisée des prestations de supervision et de management des réseaux LAN et Wi-Fi.

La réversibilité constitue une obligation contractuelle, applicable en cas de :

- Arrivée du terme du marché ;
- Résiliation, quelle qu'en soit la cause.

La réversibilité porte notamment sur :

- Les configurations, paramètres, règles, tableaux de bord et alertes ;
- Les données d'exploitation, historiques, journaux, rapports et métadonnées ;
- La documentation technique et fonctionnelle relative aux prestations ;
- Toute information nécessaire à la continuité de la supervision et du management des infrastructures réseaux.

À la demande du pouvoir adjudicateur, le titulaire devra :

- Transmettre l'ensemble des données et informations dans des formats exploitables, standards ou couramment utilisés sur le marché ;
- Fournir une documentation complète, à jour et intelligible, permettant la reprise des prestations ;
- Assurer une assistance technique et fonctionnelle pendant la période de réversibilité, incluant des échanges avec les équipes du pouvoir adjudicateur ou du nouveau prestataire ;
- Répondre aux sollicitations nécessaires à la bonne compréhension de l'existant.

Le titulaire s'engage à maintenir les prestations en conditions opérationnelles pendant toute la durée de la réversibilité, jusqu'à la prise d'effet complète de la solution de remplacement ou de la reprise en interne, sauf décision contraire du pouvoir adjudicateur.

Les opérations de réversibilité devront être conduites dans le respect :

- Des règles de sécurité des systèmes d'information ;
- Des obligations de confidentialité prévues au marché ;
- De la réglementation applicable en matière de protection des données.

À l'issue de la réversibilité, le titulaire procédera, sur demande du pouvoir adjudicateur, à la suppression ou restitution de toutes les données détenues, et en attestera par écrit.

Les prestations de réversibilité sont réputées incluses dans les prix du contrat.

Toute prestation supplémentaire fera l'objet d'un accord préalable écrit du pouvoir adjudicateur.

Le titulaire est pleinement responsable de la bonne exécution de la réversibilité.

Toute carence ou manquement pourra entraîner l'application des pénalités prévues au marché, sans préjudice des autres droits du pouvoir adjudicateur.