# CAHIER DES CLAUSES TECHNIQUES PARTICULIERES

## PRESTATIONS D'ASSISTANCE, DE MAINTENANCE ET DE DEVELOPPEMENT SUR LE SITE LES AIDES.FR

*Réf. marché : CCIR-COM-2026-59*

hautsdefrance.cci.fr

299 boulevard de Leeds - CS 90028 - 59031 LILLE CEDEX
T. 03 20 63 79 79

CCI HAUTS-DE-FRANCE

# ARTICLE 1. OBJET DE LA CONSULTATION ET DISPOSITIONS GENERALES

Le présent marché a pour objet la maintenance préventive, corrective, adaptative et évolutive du site national d'information sur les aides aux entreprises, Les-aides.fr

La CCI Hauts-de-France pourra être amenée à demander de nouveaux développements qui ne sont aujourd'hui pas identifiés précisément. Chaque fonctionnalité fera l'objet d'une demande spécifique détaillée qui se traduira par la proposition d'un devis spécifique par le candidat.

L'hébergement des plateformes n'est pas compris dans ce marché. Toutefois, en cas de besoin, le prestataire doit passer par une demande à la DSI.

**La prestation consiste alors à :**

- analyser l'expression des besoins
- conseiller et mettre en œuvre les évolutions pertinentes
- produire une documentation technique et fonctionnelle
- fournir ensuite les montées en version de la solution

## 2.1. Durée

### a. Durée de l'accord cadre

Le marché est conclu pour une durée ferme de 12 mois à compter de sa notification

Le marché sera reconductible 3 fois par tacite reconduction pour une période de 12 mois, soit une durée globale de 48 mois maximum.

En cas de non-reconduction, le titulaire se verra notifier une décision par voie expresse au minimum 2 mois avant la date anniversaire de l'accord cadre.

La reconduction intervient :

- Au plus tôt à compter de la date de notification du bon de commande qui provoque le dépassement du montant maximum périodique
- Au plus tard au terme d'un délai d'un an à compter de la date de notification du marché

La CCI prendra par écrit la décision de ne pas reconduire l'accord-cadre sous réserve de prévenir le titulaire par écrit au plus tard trois mois avant la date anniversaire du marché public. En cas de non-reconduction, la CCI n'est pas tenue de fournir les motifs au titulaire.
Date prévisionnelle de notification : janvier 2027

**Modalités de reconduction :**
Le contrat est reconduit de manière tacite. L'acheteur notifie la décision de ne pas reconduire le contrat 2 mois avant la date de fin de la période d'exécution en cours.
Le titulaire ne peut pas refuser la décision de reconduction du contrat.

### b. Durée d'exécution

**Durée maximale d'exécution :**

- 12 mois pour la maintenance préventive, corrective et adaptative, mises à jour fonctionnelle et technique. Assistance sur la solution (bons de commande)
- 6 mois pour les autres prestations (marchés subséquents)

Le délai court à compter de la date prescrite par le bon de commande/marché subséquent ou, à défaut, à compter de la réception du bon de commande/marché subséquent par le titulaire.

# ARTICLE 2. DESCRIPTION DU SITE OBJET DE L'ACCORD CADRE

Les-aides.fr est le site d'information des CCI (Chambres de Commerce et d'Industrie) sur les aides aux entreprises.

Les-aides.fr est géré et administré par la CCI Hauts-de-France, pour le compte du réseau des CCI de France. Le site Les-aides.fr fait partie des outils reconnu produit de portée nationale par le réseau des CCI.

Le site Les-aides.fr est accessible par les URL suivantes : https://les-aides.fr (connexion sécurisée).

L'ensemble est la propriété de la seule CCI Hauts-de-France.

La CCI Hauts-de-France gère depuis 2003 un site d'information sur les aides aux entreprises, pour le compte du réseau des CCI. Le site Semaphore (www.semaphore.cci.fr ) a existé de 2003 à fin 2013. Le site Les-aides.fr a été mis en ligne en avril 2011. Début novembre 2013, le site Les-aides.fr est devenu le site unique d'information des CCI sur les aides aux entreprises, faisant ainsi la synthèse entre les fonctionnalités implantées sur l'ancien site Semaphore et sur le site Les-aides.fr.

Le site Les-aides.fr a réalisé en 2025 les audiences suivantes :

- 677162 visites,
- 1 491 154 de pages vues,
- 270 740 requêtes d'utilisateurs pour identifier les aides et financements mobilisables pour leur projet d'entreprise.

## 2.1 Description du contenu du site Les-aides.fr

Le site Les-aides.fr publie 2 types de contenu :

- Le descriptif des aides aux entreprises. Ces dispositifs d'aides couvrent toutes les activités (industrie, commerce, services, café-hôtel-restaurant, agriculture) toutes les thématiques (innovation, développement durable, production-qualité-sécurité, international, ressources humaines, prévention des difficultés, création, transmission, reprise, etc.), tous les profils (chef d'entreprise, créateur, repreneur, cédant), tous les moyens d'intervention (aides financières publiques et privées, accompagnements techniques publics et privés), tous les périmètres d'intervention (européen, national, régional, départemental et local),
- Un contenu rédactionnel dont la finalité est d'expliquer l'usage et l'intérêt des dispositifs d'aide ou de certaines familles de dispositifs.

Le site vise 2 lectorats :

- Le grand public qui consulte Les-aides.fr de manière connectée ou non connectée. Le grand public accède au contenu qui lui est réservé, présentant de manière sommaire les dispositifs d'aides aux entreprises. Le grand public qui consulte le site en étant connecté à son espace Membres dispose de fonctionnalités supplémentaires : enregistrement des recherches et des dispositifs préférés, inscription à des newsletters, mise en relation avec la CCI de son territoire,

- Le public Experts, composé de conseillers CCI ou de professionnels de l'accompagnement de l'entreprise. Les Experts ont accès au contenu complet de description des aides aux entreprises, de fonctionnalités de recherche détaillées, de fonctionnalités supplémentaires : enregistrement des recherches et des dispositifs préférés, inscription à des newsletters. Les-aides.fr fait ainsi partie des outils utilisés quotidiennement par les conseillers de l'ensemble des CCI de France.
-

Les-aides.fr se compose des éléments suivants :

- Une base de données, permettant de gérer le contenu descriptif des aides aux entreprises. Une partie du contenu de la base de données est alimenté par plusieurs sources externes,
- Un moteur de recherche, permettant d'exploiter le contenu de la base de données pour réponse aux recherches des internautes,
- Des contenus éditoriaux destinés à expliquer et promouvoir les aides aux entreprises,
- Une fonction Contact mail pour relations avec les utilisateurs,
- Le site les-aides.fr qui accueille l'ensemble des 4 éléments ci-dessus,
- Des formulaires de recherche en marque blanche, pouvant être intégrés sur des sites tiers,
- Un accès open data,
- Un accès webservice privé (déjà opérationnel et exploité par plusieurs sites partenaires utilisant les jeux de données),

Depuis juillet 2026, les-aides.fr dispose d'un chatbot appelé "Ophelia" permet de poser des questions en mode non connecté avec l'utilisateur.

Les-aides.fr comprend plusieurs profils d'utilisateurs identifiés.

Certains de ces profils permettent d'accéder à des sous-domaines réservés (voir ci-après) :

- Les Membres : utilisateur se connectant en tant que Grand public identifié, accédant au contenu sommaire et à des fonctionnalités supplémentaires non accessible au grand public non connecté,

- Les Experts (profil Conseiller) : utilisateur se connectant au site Les-aides.fr et ayant accès à la totalité du contenu des aides aux entreprises, des fonctionnalités de recherche détaillées et des fonctionnalités supplémentaire d'enregistrement des dispositifs. Les dossiers peuvent également être exportés en pdf.

- Les Gestionnaires : utilisateurs en charge de la gestion du contenu de la base de données, ils font partie de la cellule nationale les-aides.fr.

Le Gestionnaire National a accès à l'ensemble des fonctionnalités de l'espace Gestionnaire et à l'ensemble du contenu de la base de données : la base nationale (qui comprend les aides nationales et européennes) et l'ensemble des bases territoriales.

Le Gestionnaire National dispose automatiquement d'un profil Conseiller.

- Le Super Administrateur : cet utilisateur a accès à l'ensemble des sous-domaines qui composent le site Les-aides.fr (voir ci-après).

Le site Les-aides.fr comprend également plusieurs sous-domaines :

- L'espace Gestionnaires, qui permet aux personnes en charge de la gestion du contenu de la base de données d'accéder aux fonctionnalités réservées aux Gestionnaires : gestion du contenu éditorial, saisie des dispositifs, saisie et affectation des contacts des organismes porteurs des aides, indexation dans les différentes tables de

critères ou de thesaurus, affectation de la zone d'implantation géographique des organismes et des dispositifs, exploitation des tableaux de bord permettant le suivi du volume de données à mettre à jour selon des plannings annuels et mensuels,

- L'espace Administration, qui permet aux personnes qualifiées comme Administrateurs de gérer le contenu des tables, les profils utilisateurs, les formulaires pour insertion sur sites tiers, les statistiques de gestion de la base de données,

- L'espace Statistiques, qui permet aux Administrateurs d'accéder aux statistiques de consultation selon les différents accès au site ou à la base de données, via l'outil Awstats,
- Le webservice open data,
- Le web service privé.

## 2.2 Environnement technique

- **Serveur**

Système d'Exploitation GNU/Linux 6.12 Debian 13
Serveur HTTP Apache 2.4
Moteur de bases de données relationnelles PostgreSQL 17
Node.js v20.19

- **Accès**

URL publiques :
- https://les-aides.fr/
- https://static.les-aides.fr (dns)

URL experts :
- https://cci.les-aides.fr/
URL Services Web
− https://ws.les-aides.fr/
− https://api.les-aides.fr/
− https://srqp.les-aides.fr/

URL d'administration sécurisée :
−https://back.les-aides.fr/

- **Langages utilisés**

Langage de programmation principal :
− PHP 8.4
− Framework interne non référencé sur le marché (Sémaphore 7)

Langages de programmation complémentaires :
− SQL
− Java
− JavaScript
− Bash

Langages de données et formatage
− HTML 5
− CSS 3
− XML
− JSON

Protocoles et technologies de communication
− HTTPS
− REST/JSON
- SSH

Détection/protection

− Routage actif
− Redirections Apache
− Fail2ban

- **Quantification du code**

| | |
|---|---|
| Classes PHP : | 295 |
| Interfaces PHP : | 7 |
| Traits PHP : | 3 |
| Autres fichiers PHP : | 137 |
| Fichiers javascript : | 68 |
| Fichiers SASS : | 155 |
| Fichiers TWIG : | 148 |
| Lignes de code : ± | 240000 |
| Fichiers de configuration JSON : | 130 |
| Fichiers SQL : | 7 |

Lignes de données : ± 23000

- **Quantification des données**

| | |
|---|---|
| ± 13 Gio de | données |
| ± 7.5 Gio d'archives | compressées. |
| Schémas : | 21 |
| Tables : | 200 |
| Vues : | 36 |
| Index et clefs : | 254 |
| Relations : | 275 |
| Procédures embarquées : | 129 |

- **Architecture matérielle**

Serveur en cluster haute disponibilité : deux machines en miroir sur deux sites distincts avec bascule automatique en cas de défaillance.

− Processeur Intel Xeon 8 cœurs @ 2.30GHz
− 16 Gio RAM
− 200 Gio SSD

### 2.3 Code Legacy PHP

La base du code PHP, actuellement en 8.4 n'est pas associé à un Framework moderne ( ex Symfony, Lavarel ...) et représente un plus périlleux pour une équipe de développement dans la reprise d'un tel projet. Néanmoins, le code a toujours été maintenu pour limiter les risques et les vulnérabilités rendant le site et les services associés ( ex api ) toujours opérationnels.

Il n'est pas prévu pendant ce marché une refonte profonde du projet (changement de langage, intégration d'un Framework ou la conteneurisation) sauf en cas de nécessité lié à la sécurité ou au changement de standard imposé par la DSI. Nous sommes donc loin des promesses d'innovation et d'architecture propre véhiculées par les Frameworks modernes ou le DevOps.

### 2.4 Historique du projet

Conception initiale
2002 : Sémaphore v1

Evolutions :

2005 : Evolution BO
2009 : Evolution FO/BO (Framework v2 + Sémaphore v2)
2011 : Séparation FO grand public(les-aides.fr) / experts, réécriture BO/BDD (Framework v3 + Sémaphore v3)
2013 : Evolution FO/BO (Sémaphore v4)
2017 : Réécriture FO/BO/BDD (Framework v4 + Sémaphore v5)
2021 : Evolution FO/BO (Sémaphore v6)
2023 : Evolution FO/BO/BDD (Framework v5 + Sémaphore v7)

### 2.5 Évolutions récurrentes et ponctuelles

Evolutions récurrentes :

- mise à jour des informations géographiques (COG de l'INSEE),
- restructuration régulières et ré-indexation.
- mise à jour ou intégration des zones primables (Legifrance, JO)
- production de statistiques, consolidation
- mise à jour des accès API (data.gouv.fr, Opendata Région des pays de la Loire, INSEE),
- renouvellement des licences

Evolutions ponctuelles :

- tables INSEE (ex NAF2025 à implémenter en 2027, structure COG)
- ajout de modules (IA, WAF, ...)
- évolution de la plateforme (Apache, PHP, node, etc.)

## ARTICLE 3. **PRESTATIONS ASSUREES PAR LE TITULAIRE**

### 3.1 Tierce maintenance applicative

Il s'agit des prestations permettant le maintien en condition opérationnelle et le maintien en condition de sécurité du site internet à titre préventif ou correctif mais également dans un but évolutif et adaptatif.

Le Titulaire retenu devra mettre à disposition de la CCI Hauts-de-France un espace de gestion et de traitement des demandes de maintenance qu'il aura détaillé dans son offre. Ces demandes fonctionneront selon un système de tickets permettant aux administrateurs de Les-aides.fr de solliciter les équipes techniques en charge de la maintenance. Ce système de tickets devra permettre une graduation des demandes, selon 3 niveaux de gravité du besoin :

**- Gravité 1 - Critique** : Ce statut exceptionnel implique un traitement d'urgence et est donc réservé à des problèmes remettant en cause de manière profonde le fonctionnement du site ou de la base de données Les-aides.fr et la délivrance du service auprès de l'internaute. De par sa définition, ce statut est réservé à des environnements en exploitation ou à des environnements de qualification lors des phases de site pilote avant diffusion généralisée des produits.

**- Gravité 2 – Bloquant** : Statut correspondant à des problèmes graves de fonctionnement remettant en cause l'intégrité des données ou la réalisation de fonctionnalités majeures, sans toutefois empêcher l'accès au site ni la délivrance partielle du service à l'internaute. Ce statut implique un traitement prioritaire de la correction.

**- Gravité 3 – Gênant** : Statut correspondant à un incident non bloquant, non urgent ou permettant une procédure de contournement. C'est l'option par défaut pour tout incident. Ce statut sera également utilisé pour tout besoin de maintenance adaptative conditionné à une date limite d'exécution (ex : avoir modifié le contenu de la table X pour telle date).

A titre informatif et simplement indicatif (non contractuel), ce temps de maintenance est estimé en durée à 10 jours par an.

### 3.2 Maintenance préventive et corrective

Dans le cadre de la maintenance préventive, le prestataire veillera notamment à :

- Mettre à jour le CMS
- Mettre à jour le thème et les plugins des sites
- Nettoyer la base de données
- Veiller aux failles de sécurité
- Effectuer une sauvegarde complète et régulière des données
- Vérifier la mise à jour des extensions installées sur les sites

La maintenance corrective comprend la fourniture de correctifs ponctuels pour des éventuels dysfonctionnements ainsi que la prise en compte de toute anomalie bloquante, empêchant l'utilisation des fonctions principales de l'application et le traitement jusqu'à la résolution.

Il peut s'agir d'un problème d'ordre sécuritaire, un problème d'hébergement ou encore la non-accessibilité aux sites internet (correction de codes obsolètes, résoudre des problèmes d'affichage, corriger des failles de sécurité, corriger un dysfonctionnement par suite d'un changement d'hébergeur web, …)

### 3.3 Demandes de maintenance adaptative

Les opérations de maintenance adaptative à réaliser sur le site et la base de données Les-aides.fr pourront notamment être les suivantes :

- Mises à jour liées à l'intégration de nouveaux langages web ou de nouvelles contraintes techniques nécessitant des développements supplémentaires pour maintenir l'ensemble des fonctionnalités opérationnelles,

- Mises à jour du contenu ou de la structure de certaines tables pour s'adapter à un référentiel d'informations produit ou fourni par un tiers et impactant la structure et le contenu de la base de données (ex : début 2016, mise à jour du référentiel géographique réalisé pour s'adapter aux nouvelles régions ; adaptation de la table des communes selon les mises à jour annuelles de la table des communes de l'INSEE ; mise à jour des informations relatives aux zones aidées ; mise à jour des informations relatives aux communes à destination des utilisateurs, etc.).

- Intégration dans la structure du site ou mise à jour de modules ou outils en ligne développés par des sites tiers et intégrables en marque blanche : ex : simulateur d'embauche développé par le secrétariat général pour la modernisation de l'action publique (SGMAP),

- Modifications logicielles destinées à améliorer le fonctionnement des fonctionnalités existantes, ou à ajouter des modules supplémentaires aux fonctionnalités existantes,

### 3.4 Demandes d'évolution ultérieures (maintenance évolutive)

Les demandes d'évolution consistent en toute modification de l'application dont le but n'est pas de corriger une anomalie. Elles concernent notamment les évolutions en termes de contenu des sites et de développements de nouvelles fonctionnalités.

Pour exemple, les demandes d'évolution consisteront dans les demandes suivantes :

- Assistance technique dans la définition des fonctionnalités à créer et développées : en réponse aux demandes de l'administrateur de Les-aides.fr, définition des contraintes techniques à prendre en compte et propositions des réponses techniques les mieux adaptées,

- Création et développement de nouvelles fonctionnalités : selon les besoins, création de nouvelles fonctionnalités. Ces développements pourront concerner le site Les-aides.fr, le fonctionnement de la base de données ou du moteur de recherche, les différents sous-domaines, les besoins liés aux accès extérieurs à la base de données accordée aux partenaires, etc.

Les besoins exacts d'évolution seront spécifiés ultérieurement au titulaire du marché via les marchés subséquents.

Les candidats s'engageront sur un coût journalier par profil (chef de projet, développeur, …) qui servira de base au chiffrage de la prestation ultérieure.

### 3.5 Assistance et délais d'intervention pour la maintenance corrective

Le prestataire devra assurer l'accueil et l'assistance téléphonique (hotline).

Une disponibilité est demandée pendant les jours ouvrés du lundi au vendredi de 9h à 18h.

En ce qui concerne la maintenance préventive, le Titulaire intervient dès détection de la tentative d'attaque de l'intégrité de la base de données ou du site Les-aides.fr et informe l'administrateur Les-aides.fr dès la fin de l'intervention.

En ce qui concerne la maintenance corrective ou adaptative, le Titulaire s'engage sur les délais ci-après :

- Dans le cas d'un incident critique, le délai d'intervention ne devra pas excéder 4 heures ouvrées et le délai maximum de résolution des incidents ne devra pas excéder 8 heures ouvrées.

- Dans le cas d'un incident bloquant, le délai d'intervention ne devra pas excéder 8 heures ouvrées et le délai maximum de résolution des incidents ne devra pas excéder 24 heures ouvrées.

- Dans le cas d'un incident gênant, le délai d'intervention ne devra pas excéder 24 heures ouvrées et le délai maximum de résolution des incidents ne devra pas excéder 48 heures ouvrées.

Chacun de ces délais court à compter du signalement par écrit de l'anomalie.

Le signalement par écrit des anomalies est formalisé par l'émission d'un ticket.

Le prestataire définira dans sa réponse les points suivants :

- L'organisation globale du service de maintenance,
- La procédure de déclenchement d'une action en maintenance (mode d'appel, mode d'intervention…) ; celui-ci s'effectuera impérativement à l'aide d'un support horodaté (e-mail, site internet…).
- Les exclusions au contrat de maintenance,
- Les engagements de délais d'intervention, de résolution et de mise en place de solution de contournement

A chaque intervention, en cas d'incident, une fiche de suivi indiquant l'incident (date, heure, intervenant, …) et sa résolution sera communiquée au client dans la semaine suivant la clôture de l'incident.

En ce qui concerne les demandes de maintenance adaptative conditionnées à une date limite d'exécution, le Titulaire s'engage à avoir terminé son intervention la veille (jour ouvré) de cette date limite d'exécution.

Le Titulaire s'engage à communiquer à l'administrateur Les-aides.fr les informations nécessaires à la bonne utilisation de l'outil de suivi des demandes.

Le Titulaire s'engage à maintenir à jour la documentation technique de l'accès open data et de l'accès webservice privé.

### 3.6 Qualité de service attendu

La plateforme doit offrir des performances optimales en termes de vitesse d'affichage des pages et présenter le meilleur taux de disponibilité possible. Plusieurs milliers de connexions d'utilisateurs au site doivent pouvoir être accueillies simultanément.

Les opérations de maintenance des sites devront être effectuées au cours des plages horaires présentant le moins de trafic.

GTR : 4 heures
Fraicheur des données restaurées (RPO) : J-1
Nombre d'arrêts planifiés acceptés : 1 par trimestre
Temps de back up : 1h00

# ARTICLE 4. **GESTION DE LA SECURITE**

Le candidat précisera les moyens mis 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 suite aux insuffisances constatées lors de la vérification).

## 4.1 Mises à jour, correctifs de sécurité

Le prestataire applique les correctifs recommandés par les fournisseurs de solutions matérielles ou logicielles (logiciels système ou applicatifs, logiciels embarqués) sur l'ensemble des sites dont il a la charge.

En cas d'alerte grave (attaque virale, faille critique) annoncée par le CERTA (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 CERTA 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 prestataire 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 prestataire, par l'administration ou le CERTA, 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 prestataire 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.

## 4.2 Continuité d'activité

Le prestataire doit prendre toutes les mesures nécessaires pour assurer la disponibilité de l'application. Il 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 conformément aux exigences définies dans la clause sur la convention de service du Plan d'Assurance Sécurité.
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.

## 4.3 Authentification dans le Back Office

Pour chaque interface d'accès au système, (Interface Homme-Machine, interface entre applications) le prestataire 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.

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

## 4.5 Contrôle 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 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 notamment :

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

Le prestataire 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. Un WAF est en place sur le site les-aides.fr permettant de filtrer et analyser le trafic HTTP/HTTPS.

### 4.6 Imputabilité, traçabilité

Les informations suivantes devront être enregistrées :

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

### 4.7 Personnels en charge des prestations

Le prestataire s'engage à fournir une liste, régulièrement mise à jour, 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).

Qualifications et expérience, formations et sensibilisation dans le domaine de la SSI des personnels en charge des prestations. Le prestataire indiquera dans sa réponse :

- 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.

### 4.8 Exigences de sécurité concernant les personnels extérieurs (maintenance, audit…)

Le prestataire 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

### 4.9 Intervention des sociétés de maintenance ou de support de solutions informatiques

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 prestataire 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 applications développées restent la propriété de la CCI de de région Hauts de France.

### 4.10 Audit de sécurité

La CCI de région 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 de région 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 sont à la charge du prestataire.

### 4.11 Controle des prestations fournies

Le Titulaire est tenu de présenter au Pouvoir Adjudicateur les prestations dans les conditions prévues au présent CCP.

La maintenance corrective comprend des activités telles que :

- Le diagnostic
- L'ouverture d'un ticket d'incident
- La réalisation de corrections
- La mise en place de solutions de contournement
- La mise à jour de la demande sur un portail et son statut afin de partager son état

Le principe de fonctionnement est le suivant :

- Une demande de correction est émise par le service via une fiche d'anomalie
- Le problème est qualifié par l'équipe du prestataire qui en vérifie la priorité, définit la solution de contournement si nécessaire et le délai de résolution
- un plan d'actions est communiqué à l'émetteur de la demande
- la correction de l'anomalie est réalisée dans le délai requis en fonction des niveaux de service spécifiés
- le statut de la demande est mis à jour en fonction de son traitement

Une fois par mois, le prestataire fournira un compte-rendu d'activité faisant état des anomalies (ticket d'incidents ouverts, en cours, clos)- avec la date et l'heure de signalement des anomalies et des plans d'actions associées.

Le Titulaire fournira également un compte-rendu pour les prestations assurées au titre de la maintenance préventive, de l'assistance (téléphone ou courriel) et de la maintenance adaptative.

Pour toutes les prestations assurées au titre de la maintenance adaptative, un relevé de réalisation des opérations devra être alimenté.

Pour les prestations de maintenance évolutive ou de développement de nouvelles fonctionnalités, une documentation technique précisant notamment les éventuelles contraintes d'utilisation (version de navigateur, etc.), les impacts ou articulations avec une autre fonctionnalité, les mises à jour de table nécessaires, etc, devra être fournie. Les prestations d'assistance technique pour la définition des fonctionnalités à développer donneront lieu à l'établissement d'une note technique du titulaire détaillant le contenu et la durée de la prestation. Avant tout début d'exécution, les préconisations du titulaire devront avoir fait l'objet d'un accord exprès de la CCI Hauts-de-France qui sera formalisé par l'établissement du bon de commande.