
CAHIER DES CLAUSES TECHNIQUES PARTICULIERES

CCTP

MARCHE PUBLIC RELATIF AUX PRESTATIONS D'INFOGERANCE ET D'HEBERGEMENT DU SYSTEME INFORMATIQUE DE L'AGENCE FRANÇAISE DE LUTTE CONTRE LE DOPAGE

Contents

1	INTRODUCTION	6
1.1	AFLD, Contexte et Objectifs	6
1.2	Définition du système Informatique de l'AFLD	6
1.3	Objet du marché, périmètre	6
2	DISPOSITIF DU MARCHE.....	7
3	DESCRIPTION DU SYSTEME INFORMATIQUE AFLD	8
3.1	Fonction informatique et parties prenantes du système informatique AFLD	8
3.1.1	Le responsable système d'information.....	8
3.1.2	Le prestataire infogérant, titulaire du(des) lot(s) correspondant(s).....	9
3.1.3	Le prestataire Hébergeur, titulaire du (des) lot(s) correspondant(s)	9
3.1.4	Les utilisateurs AFLD et la MOA AFLD	9
3.2	Présentation du système informatique AFLD	10
3.2.1	Architecture technique du réseau AFLD	10
3.2.2	Description des systèmes infogérés, modalités des sauvegardes	13
3.2.3	Réseau sans fil AFLD.....	13
3.2.4	Les applications & serveurs hébergées de l'agence	13
3.2.5	Le parc de postes informatiques.....	15
3.2.6	Evolutions prévisibles du système informatique	15
3.2.7	Local technique de l'AFLD	15
3.2.8	Gestion des noms de domaine AFLD	16
3.2.9	Sécurité du système d'information de l'AFLD : exigences minimales de l'AFLD	16
3.2.10	Schéma simplifié, organisation hébergement versus infogérance.....	18
4	LOT 1 – Prestation de services pour l'infogérance du système informatique de l'AFLD.....	19
4.1	Mise en place / Phase de cadrage : prestation forfaitaire F01 (réversibilité entrante)	19
4.1.1	Transfert des prestations	19
4.1.2	Note de cadrage & réunion de lancement, PAQ, et PAS	19
4.2	Infogérance en mode opérationnel – prestation forfaitaire F02.....	20
4.2.1	Périmètre de départ de l'infogérance, systèmes du SI AFLD.....	21
4.2.2	Support aux utilisateurs – Prestation forfaitaire F03.....	22
4.2.2.1	Prestations attendues du support de niveau 2 et 3 et son périmètre.....	22
4.2.2.2	Traitement des demandes, résolution des incidents.....	23
4.2.2.3	Accessibilité du support infogérant	24
4.2.3	Maîtrise d'œuvre et pilotage de l'infogérance – prestation forfaitaire F04.....	24

4.2.3.1	Pilotage de l’infogérance, SDM, ROC : interlocuteurs exigés dans le cadre de la prestation	25
4.2.3.2	Devoir d’alerte, de conseil	25
4.2.3.3	Plan d’Assurance Qualité	26
4.2.3.4	Plan d’assurance sécurité – PAS.....	27
4.2.3.5	Comités	27
4.2.3.6	Comité technique.....	28
4.2.3.7	Comité de pilotage.....	28
4.2.3.8	Comité Innovations et Evolutions	29
4.2.3.9	Documentation, mise à jour constante	30
4.2.4	L’administration et l’exploitation des systèmes	30
4.2.4.1	Généralités.....	30
4.2.4.2	Description des prestations	31
4.2.5	La gestion de la messagerie électronique.....	32
4.2.6	La gestion des changements informatiques	32
4.2.7	Prestations annexes	32
5	LOT 2 – Prestation de services pour l’hébergement du système informatique de l’AFLD, services et fournitures des liens de connexions avec le data center	34
5.1	Périmètre de la prestation d’hébergement et FAI	34
5.1.1	Socle de l’infrastructure de départ	34
5.1.2	Liens de communications (F03 – COMM INSTALL)	36
5.1.3	Exigences particulières pour le titulaire et le choix de son opérateur fibre dans le cas de l’offre de base	36
5.1.4	Exigences particulières pour le titulaire et le choix de son opérateur fibre : variante à la proposition précédente.....	37
5.1.5	Nomadisme et accès au système d’information de l’AFLD.....	38
5.1.6	Dispositifs de sécurité de l’hébergeur	38
5.1.7	Licences Microsoft Windows, serveur & CAL.....	39
5.2	Mise en place / Phase de cadrage / Plan de migration & Migration vers nouvelle infrastructure – prestation forfaitaire F01-HEB	39
5.2.1	Transfert des prestations	39
5.2.2	Note de cadrage, PAQ, réunion de lancement et plan de migration	40
5.3	Hébergement en mode opérationnel – prestation forfaitaire F02-HEB (T1)	41
5.3.1	Maitrise d’œuvre et pilotage de l’hébergement du SI.....	41
5.3.1.1	Pilotage de l’hébergement, interlocuteurs exigés dans le cadre de la prestation	41
5.3.1.2	Devoir d’alerte, de conseil	42

5.3.1.3	Plan d'Assurance Qualité	43
5.3.1.4	Plan d'assurance sécurité – PAS.....	43
5.3.1.5	Comités	43
5.3.1.6	Comité de pilotage	44
5.3.1.7	Reporting.....	45
5.3.1.8	Validation des installations tierces	45
5.3.1.9	Documentation, mise à jour constante	46
5.3.2	Evolution du SI AFLD, Déploiement de nouvelle VM	46
5.3.3	L'administration et l'exploitation des systèmes	47
5.3.3.1	Généralités	47
5.3.3.2	Description des prestations	47
5.3.4	L'administration et l'exploitation des réseaux.....	49
5.3.4.1	Généralités	49
5.3.4.2	Description des prestations	49
5.3.5	La gestion des changements informatiques	50
5.3.6	La supervision des systèmes et des réseaux.....	50
5.3.7	Prestations annexes	50
6	Convention de services, disponibilité et réversibilité applicable à tous les lots.....	52
6.1	Disponibilité du système informatique	52
6.2	Résolution d'incident	52
6.3	Limite de responsabilité.....	52
6.4	Niveau de service constaté et niveau de service garanti.....	52
6.5	Heures de service normales	52
6.6	Heures de service étendues	52
6.7	Criticités des applications	53
6.8	Indicateurs de la disponibilité.....	53
6.8.1	Mesure de la disponibilité.....	53
6.8.2	Définition des arrêts planifiés	54
6.9	Engagement de disponibilité de l'infrastructure et des applications, exigence sur les sauvegardes, exigence d'évolutivité et de liaison entre les sites.....	54
6.9.1	Politique de sauvegarde des données AFLD	54
6.9.2	Exigences de disponibilité, d'évolutivité et d'un site de secours	55
6.9.3	Plan PRA, Vérification, tests, suivi du plan.....	56
6.10	Phase de réversibilité	56
6.10.1	Garantie de réversibilité	56

6.10.2	Création et mise à jour.....	56
6.10.3	Contenu.....	56
6.10.4	Obligations de fin de l'accord-cadre	57
6.10.5	Mise en œuvre	57

1 INTRODUCTION

1.1 AFLD, Contexte et Objectifs

L'Agence française de lutte contre le dopage (AFLD) est une autorité publique indépendante chargée de définir et de mettre en œuvre les actions de lutte contre le dopage dans le sport. Elle remplit à cet effet des missions d'éducation, de prévention, de contrôle, de réglementation et de sanction. Elle coopère également au niveau international avec l'Agence mondiale antidopage et avec les organisations antidopage signataires du code mondial antidopage.

L'AFLD s'inscrit depuis plusieurs années dans une importante dynamique de transformation et se développe dans tous les domaines de son activité.

Les événements sportifs internationaux passés et futurs (RUGBY2023, JOPPARIS2024, JO2030...), les projets stratégiques de l'AFLD (investigation sur les données massives, services numériques renforcés, dématérialisation des processus métiers...) sont des rendez-vous et des enjeux très importants pour l'AFLD et ont de près ou de loin des impacts sur la stratégie de son système d'information.

Le système informatique de l'entité exige un hébergement et une infogérance de très haute qualité. L'expertise, la qualité, l'accompagnement et le professionnalisme du titulaire infogérant et du titulaire hébergeur sont particulièrement attendues tout au long du marché et plus particulièrement lors de grands événements sportifs.

La nature des données manipulées au sein du SI AFLD est de fait particulièrement sensible (données personnelles, données médicales) et l'exigence porte autant sur l'intégrité de la donnée stockée, la robustesse et la sécurité du système informatique pris en charge par les prestataires.

1.2 Définition du système Informatique de l'AFLD

Pour l'exécution du présent Accord-Cadre, le système Informatique (SIn) de l'AFLD est défini comme l'ensemble des éléments matériels et logiciels informatiques de l'Agence : serveurs, postes de travail portables et fixes, logiciels serveur, logiciels clients, périphériques informatiques tels que clavier, souris..., éléments actifs tels que routeurs, switch ; contrôleurs Wi-Fi, contrôleur d'accès réseau ; système de téléphonie IP (matériel inclus).

Le système d'information (SI), quant à lui, est un ensemble plus global composé des matériels, logiciels, données, mais aussi les personnels et les procédures – permettant ainsi de coordonner les activités de l'AFLD et de son organisation afin de l'aider à atteindre ses objectifs stratégiques et opérationnels.

Ainsi, le SI englobe le SIn ; ce dernier reposant sur les technologies de l'information et de la communication.

1.3 Objet du marché, périmètre

Le présent accord-cadre a pour objet l'infogérance de l'ensemble du système informatique de l'AFLD ; l'hébergement du système informatique de l'Agence, la fourniture des liens de communication nécessaires entre l'AFLD, les data centers et l'internet. Les prestations comprennent donc :

- La prise de connaissance du SI de l'AFLD ;
- Le maintien du Système Informatique en conditions opérationnelles en garantissant les niveaux de services spécifiés ;

- La prise en charge de toute évolution de l'infrastructure rendue nécessaire par les niveaux de services spécifiés ;
- La prise en charge de toute évolution logicielle ou matérielle de l'infrastructure rendue nécessaire par l'activité de l'Agence ;
- La garantie de la sécurité des données (intégrité des données, disponibilité, sauvegarde et restauration) ;
- L'administration, l'exploitation et la supervision de dispositifs de sécurité [parefeu HA sur site Paris, parefeu HA sur DC hébergeur, passerelle de sécurité messagerie, détection & réponse des menaces sur les serveurs hébergés] ;
- L'hébergement certifié HDS de l'infrastructure SI de l'AFLD ;
- Les liens de communications sécurisés entre AFLD, son data center et internet ;
- Le fonctionnement et le support technique N2 & N3 à un niveau élevé de qualité ;
- L'administration, l'exploitation et la supervision des serveurs et du réseau AFLD ;
- La supervision d'une partie des équipements internes AFLD, au sein de l'agence (commutateurs, serveur physique) ;
- L'apport de compétences en matière de conseil et de veille technologique ;
- La maîtrise d'œuvre et le pilotage de l'infogérance ; la maîtrise d'œuvre et le pilotage de l'hébergement ;
- La réversibilité des services à tout moment ;
- Le reporting notamment du suivi de l'activité par l'intermédiaire d'indicateurs pertinents.

Ce qui est exclu du périmètre :

La gestion, l'administration, l'exploitation ou le maintien en condition opérationnelle des dispositifs internes au sein de l'agence sont exclus du périmètre des prestations. Les postes clients, les bornes wifi, les commutateurs de distribution internes sont de la responsabilité de l'AFLD.

Le support utilisateur N1.

2 DISPOSITIF DU MARCHÉ

Ce marché est composé de deux lots de prestations.

Chaque lot présenté dans ce cahier des charges est conclu pour une durée de 1 an renouvelable 3 fois sans que la durée totale n'excède 48 mois.

Disposition par lots

Référence du lot	Libellé du lot
Lot 1	Prestation de services pour l'infogérance du système informatique de l'AFLD
Lot 2	Prestation de services pour l'hébergement du système informatique de l'AFLD et fournitures des accès de communication (FAI)

La date prévisionnelle de démarrage des prestations est début mai 2025.

3 DESCRIPTION DU SYSTEME INFORMATIQUE AFLD

3.1 Fonction informatique et parties prenantes du système informatique AFLD

Les parties prenantes à ce marché sont nombreuses mais peuvent être classées de la façon suivante :

La fonction informatique clef (maîtrise d'ouvrage) au sein de l'AFLD est composée au 1^{er} janvier 2025:

- Du responsable système d'information,
- Du chargé de mission technique informatique.

Les autres parties prenantes sont :

- L'ensemble des collaborateurs AFLD qui utilise au quotidien le système informatique de l'Agence et les services d'infogérance associés,
- Les collaborateurs AFLD qui participent à la maîtrise d'ouvrage de certaines applications métiers AFLD,
- Le prestataire infogérant (parfois également appelé « le gestionnaire AFLD » dans la suite de ce document) lui-même qui maintient et exploite le système d'information,
- Les équipes projet des partenaires extérieurs à l'AFLD (Réseau des préleveurs, Ministère des sports, ...) qui accèdent à certaines ressources du système d'information de l'AFLD (sites collaboratifs, applications métiers...),

3.1.1 Le responsable système d'information

Le Responsable Système d'Information, est le garant de l'alignement du Système d'Information (SI) sur la stratégie de l'AFLD, il coordonne la mise en œuvre du schéma directeur du système d'Information dans l'objectif de maximiser la contribution du SI à la performance de l'Agence. Il évalue et préconise les investissements en fonction de l'état de l'art du marché. Il veille à l'efficacité et à la maîtrise des risques liés au système d'information.

Sous l'autorité du Secrétaire Général, en lien avec les directeurs des départements (juridique, enquêtes et investigation, contrôles, éducation et prévention), il assure le secrétariat du comité de pilotage du SI chargé de la conception et du déploiement des évolutions du système d'information.

Le chargé de mission technique et le RSI valident l'architecture technique du système d'information de l'AFLD et garantissent la cohérence des moyens informatiques, dans le cadre du schéma directeur et selon les axes définis par la direction. Ils pilotent les projets « infrastructure SI » de l'AFLD et s'assurent du suivi et du pilotage des différentes prestations SI engagées via les projets AFLD. A ce titre, ils assurent l'interface opérationnelle avec le titulaire ; ils assurent également le suivi des différents contrats/achats liés au système informatique.

Enfin, le chargé de mission technique informatique assure la gestion et l'exploitation courante des postes clients déployés aux salariés [configuration des postes, déploiement, paramétrage, intégration dans le domaine, inventaire, support aux utilisateurs etc...]. **Ces actions ne sont donc pas du ressort de l'infogérant.**

3.1.2 Le prestataire infogérant, titulaire du(des) lot(s) correspondant(s)

Par le présent accord-cadre qui le lie à l'AFLD, le titulaire est responsable d'un périmètre qui couvre :

- Le maintien en condition opérationnelle du système d'information utilisé pour le traitement des données de l'AFLD ;
- L'administration et l'exploitation du système d'information contenant les données de l'Agence ;
- La prise en charge de la transformation des dispositifs du système informatique pour répondre aux exigences de qualité de service et pour répondre aux évolutions apportées par les projets de l'Agence ;
- L'apport de son expertise et sa fonction de conseil en lien avec le RSI AFLD quant aux évolutions du système d'information de l'entité ; l'accompagnement en la matière lors de la mise en œuvre de nouvelles évolutions.

3.1.3 Le prestataire Hébergeur, titulaire du (des) lot(s) correspondant(s)

Par le présent accord-cadre qui le lie à l'AFLD, le titulaire est responsable d'un périmètre qui couvre :

- La mise à disposition et le maintien en condition opérationnelle des sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des données de l'Agence de lutte contre le dopage ;
- La mise à disposition et le maintien en condition opérationnelle des liens de communications réseaux nécessaires au fonctionnement des sites ;
- La mise à disposition et le maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de l'AFLD ;
- La mise à disposition et le maintien en condition opérationnelle des machines (serveurs) physiques et virtuelles nécessaires au fonctionnement des services SI de l'entité ;
- La mise à disposition et le maintien en condition opérationnelle des dispositifs de sécurité (physiques et/ou virtuels) nécessaires à la protection des accès au SI AFLD (Parefeux, AntiSpam, Anti virus et menaces...) ;
- L'apport de son expertise et sa fonction de conseil en lien avec le RSI AFLD et indirectement avec l'infogérant lors de la mise en œuvre de projets d'évolutions des dispositifs composant le système d'information de l'AFLD.

3.1.4 Les utilisateurs AFLD et la MOA AFLD

Les agents de l'AFLD représentent aujourd'hui 50 personnes environ sur un seul site (Paris Auber) ; ce nombre ne devrait pas évoluer davantage dans les prochaines années. Les collaborateurs AFLD sont majoritairement des personnes mobiles. Ils interagissent quotidiennement avec le système informatique via notamment l'accès à leur messagerie, aux portails collaboratifs et aux serveurs de données.

Les collaborateurs AFLD, en majorité, ont des compétences basiques dans le domaine informatique ; ils utilisent principalement les outils bureautiques office comme outil de travail.

3.2 Présentation du système informatique AFLD

La présentation ci-après représente la configuration actuelle et l'environnement technique en place au sein des data centers du prestataire infogérant actuel. Elle est susceptible d'évoluer, à la marge, au cours de 2025 et avant notifications des lots. L'éventuelle mise à jour de la configuration du SI sera transmise et annexée à ce cahier des charges.

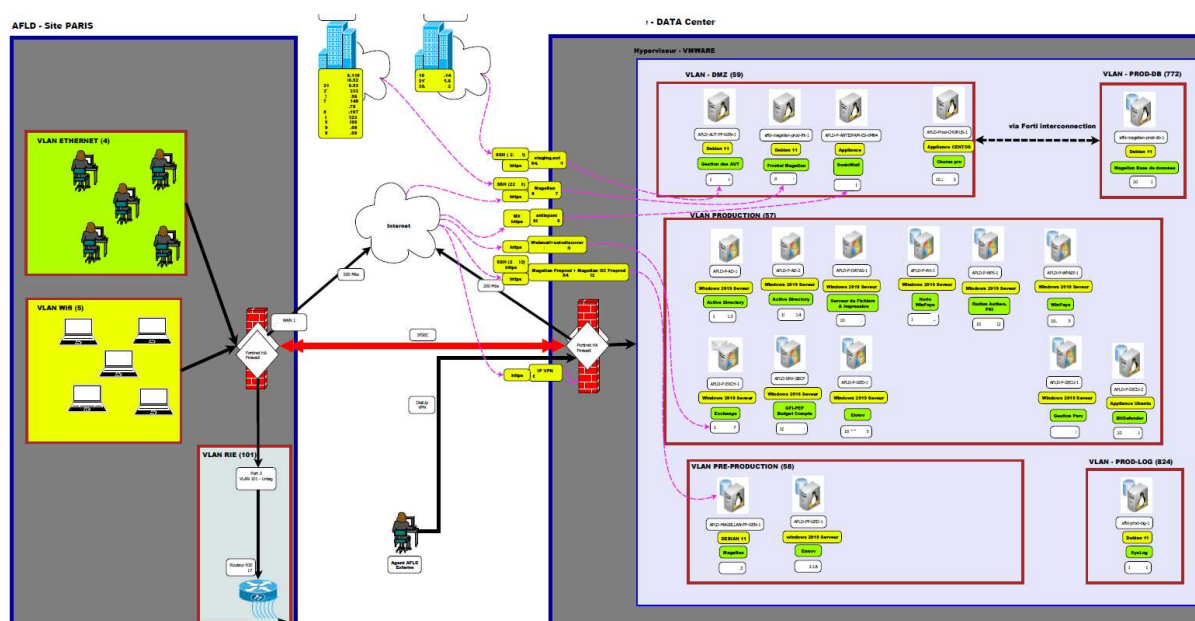
3.2.1 Architecture technique du réseau AFLD

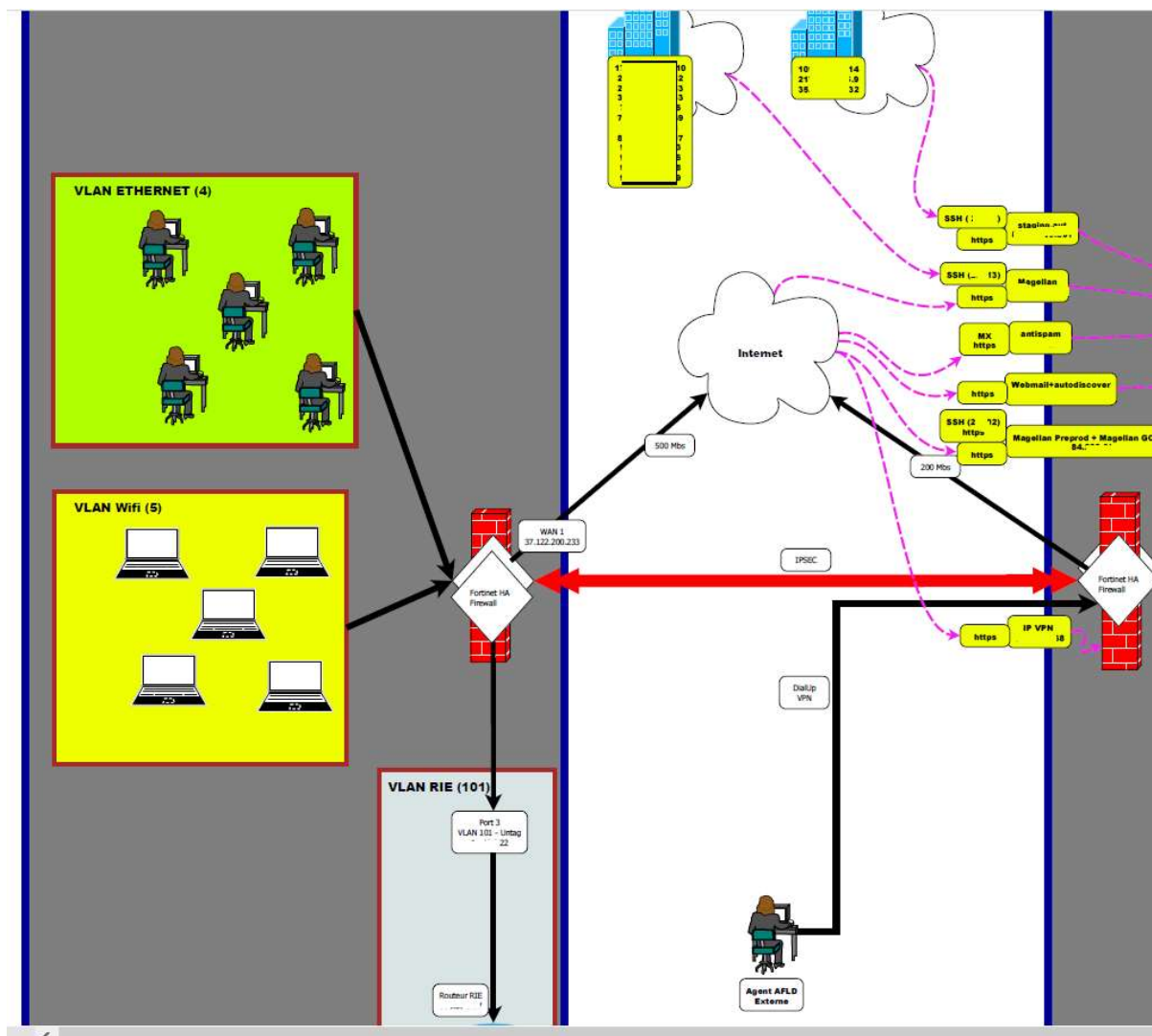
Les collaborateurs AFLD sont situés à Paris 75009. Le site est interconnecté via 1 ligne fibre FFTO MPLS 500Mb/s (liaison privée débit garanti) aux data centers du prestataire informatique actuel ; unique prestataire à la fois infogérant et hébergeur HDS.

Cette ligne fibre est fournie par le partenaire de l'hébergeur actuel.

Il assure par ailleurs une sortie sur internet d'un débit garanti de 200 Mb/s.

Cette installation fibre actuelle est fournie contractuellement par la société en charge de l'hébergement du SI de l'entité. De plus, le marché couvre la fourniture et la supervision des équipements routeurs (réparation, remplacement).





3.2.2 Description des systèmes infogérés, modalités des sauvegardes

Une description schématique du système informatique AFLD est donnée ci-dessous. L'architecture technique s'appuie sur les technologies systèmes suivantes mise en place par l'infogérant actuel :

- Active Directory Microsoft niveau domaine et forêt à jour
- Plateforme ESXi / VCenter de virtualisation des systèmes/machines
- Pare-feu Fortigate sur le DC hébergeur, haute disponibilité (x2) dédiée AFLD
- Plateforme antivirus sur tous les serveurs
- Plateforme de supervision de l'infogérant
- Plateforme antispam
- Plateforme de sauvegarde Veeam

Les sauvegardes sont gérées depuis un serveur VEEAM géré par l'hébergeur.

Il est hors du domaine AFLD et **suit les principes des règles de sécurité de l'ANSSI** concernant les sauvegardes des données :

- Serveur de sauvegarde cloisonné, et hors réseau de production de l'AFLD
- Serveur hors domaine windows (AD) de production
- Les flux de sauvegarde transitent au sein du réseau spécifique d'administration de l'hébergeur
- Règle 3-2-1 : 3 copies de sauvegarde sur 2 supports différents dont 1 hors ligne
- Les comptes admin pour la sauvegarde sont nominatifs et dédiés

La première sauvegarde hebdomadaire de l'année civile est copiée sur bandes LTO et envoyée à l'Agence Française de Lutte contre le Dopage.

L'Agence conserve ces bandes pour une durée de 10 ans

3.2.3 Réseau sans fil AFLD

L'Agence dispose d'un réseau sans fil pour ses collaborateurs. Le SSID permet :

- la connexion au réseau AFLD des postes informatiques (ordinateurs) du domaine

Des bornes wifi CISCO 2702i AC sont installées aux 2 étages de l'Agence pour une couverture optimale. Un serveur RADIUS assure l'authentification des connexions sur le réseau de l'AFLD.

Un portail captif est également disponible au sein de l'Agence et répond aux besoins de connexion à l'internet pour les invités extérieurs de l'agence. Le réseau mis en place est fourni par un routeur d'un opérateur distinct de ce marché et est donc totalement étanche au réseau AFLD de production.

3.2.4 Les applications & serveurs hébergées de l'agence

Les applications actuellement installées sont réparties sur les différentes machines virtuelles et physiques de l'infrastructure. La liste donnée ci-après n'est pas exhaustive mais recense les principales machines utilisées au sein de l'AFLD.

RQ : les machines virtuelles ou physiques sont fournies par le prestataire infogérance actuel.

RQ 2: Le descriptif ci-après reflète la situation au moment de l'écriture du cahier des charges. Il sera repris et éventuellement amendé au moment de l'installation du titulaire.

Hyperviseur	Machine Virtuelle	En Cluster	fonction	OS
POOL infogéreur	AD1	Oui	Contrôleur de domaine, AD, DHCP, DNS	Windows Server Standard, supporté, à jour
POOL infogéreur	AD2	Oui	Contrôleur de domaine, AD, DHCP, DNS	Windows Server Standard, supporté, à jour
POOL infogéreur	HOR	Non	Plateforme de gestion des congés et de paie legacy	Windows sdt supporté à jour
Pool infogéreur	AFLD-P-WPAIE-1	Non	Plateforme de gestion de la paie, metier	Windows sdt supporté à jour
POOL infogéreur	AFLD-SRV-CHORUS	Non	Interface serveur GBCP et plateforme externe CHORUS, metier	CentOS Linux
POOL infogéreur	AFLD-SRV-GBCP	Non	Serveur de gestion comptable et budgétaire, metier	Windows sdt supporté à jour
POOL infogéreur	oui	Non	Serveur de fichiers AFLD	Windows sdt supporté à jour
POOL infogéreur	oui	Non	Serveur de messagerie exchange, BAL & transport	Windows Server Standard, supporté, à jour
POOL infogéreur	AFLD-P-GED-1	Non	Serveur gestion qualité , metier	Windows Server Standard, supporté, à jour
POOL infogéreur	oui	Non	Serveur Radius Paris, NPS Authentification racine	Windows Server Standard, supporté, à jour
POOL infogéreur	oui	Non	Serveur de gestion du parc SI afd, glpi	Windows Server Standard, supporté, à jour
POOL infogéreur	oui	Non	Appliance dédiée pour solution antiviral des postes clients AFLD	Ubuntu LTS
Pool infogéreur	oui	Non	Serveur applicatif	Debian GNU/Linux
Pool infogéreur	oui	Non	Serveur applicatif métier, controle	Debian GNU/Linux
Pool infogéreur	oui	Non	Serveur applicatif, db metier controle	Debian GNU/Linux
Pool infogéreur	oui	Non	Serveur de pre production applicatif, metier controle	Debian GNU/Linux
Pool infogéreur	oui	Non	Serveur de preproduction applicatif, qualite metier	Windows Server Standard, supporté, à jour

3.2.5 Le parc de postes informatiques

Le parc est composé à 98% de portables informatiques. Un effort d'harmonisation a été entrepris, une marque est essentiellement déployée :

- Marque Lenovo X390, L13..
- Système d'exploitation : Windows 10/11 Pro (64 bits)
- Année d'acquisition
 - o La plupart des postes ont moins de 4 ans

3.2.6 Evolutions prévisibles du système informatique

Plusieurs projets d'évolution métier ou de fonctionnement sont prévus à court terme. Ils pourront apporter de nouveaux applicatifs ou de nouveaux dispositifs que devra prendre en charge le système informatique de l'AFLD, en capacité de maintien en condition opérationnelle et en capacité d'hébergement d'infrastructure évolutive.

L'infrastructure proposée par le candidat à ce marché doit permettre ces évolutions normales de la vie d'un SI sur une période longue (durée maximale du marché)

- Projet de migration/renforcement du système de messagerie,
- Projet de business Intelligence, reporting
- Projet de data sciences (analyse des données multi sources et multi formats, réseaux, data visualisation)
- .../...

3.2.7 Local technique de l'AFLD

L'AFLD dispose d'un local technique qui lui permet d'héberger les éléments nécessaires à la distribution du réseau au sein de son site (routeur principal, switches de distribution, baie de brassage) :

Il est ainsi équipé des commutateurs suivants supervisés (simple ping) par le prestataire infogérant actuel :

Nom du commutateur	Situation	Marque / brand
AFLD-SW-PA-01	Paris	Aruba 2530 POE 24
AFLD-SW-PA-02	Paris	Aruba 2530 POE 24
AFLD-SW-PA-03	Paris	Aruba 2530 POE 24
AFLD-SW-PA-04	Paris	Aruba 2530 POE 24
AFLD-SW-PA-05	Paris	Aruba 2530 24p
AFLD-SW-PA-06	Paris	Aruba 2530 24/48p

Cette supervision reste dans le périmètre des actions attendues par le titulaire du lot infogérance.

3.2.8 Gestion des noms de domaine AFLD

L'ensemble des noms de domaines AFLD publics est administré par l'AFLD sur un portail d'accès GANDI.

3.2.9 Sécurité du système d'information de l'AFLD : exigences minimales de l'AFLD

Engagement général minimal que doit fournir le titulaire du présent marché en matière de sécurité

La plate-forme d'hébergement du titulaire a vocation à héberger tout ou partie du SI de l'AFLD. À ce titre, elle doit garantir à l'AFLD sa conformité à la politique de sécurité des Systèmes d'Information (PSSIE) publiée le 17 Juillet 2014 par l'ANSSI.

Le titulaire doit respecter scrupuleusement les contraintes de sécurité exposées dans la PSSIE ainsi que dans le guide « Externalisation des SI » émis par l'ANSSI et transmis disponible sur le site officiel

<https://cyber.gouv.fr/publications/>

En outre, le titulaire s'engage à privilégier l'utilisation de solutions labellisées par l'ANSSI notamment au titre du référentiel d'exigences SecNumCloud (Niveau Essentiel, v 3.2 du 8/03/2022 ou toute autre version plus récente).

<https://cyber.gouv.fr/sites/default/files/document/secnumcloud-referentiel-exigences-v3.2.pdf>

Le titulaire produit dans son dossier technique remis au titre d'offre sa politique de sécurité SI. Il s'engage à tout mettre en œuvre pour garantir la confidentialité, l'intégrité et la disponibilité des données de l'AFLD. La plate-forme d'hébergement cloud pourra héberger des données à caractères nominatifs.

Respect de la législation française en matière d'hébergement de données de Santé

Au regard de certaines activités spécifiques à caractère médicale réalisées par l'AFLD, la plateforme technique d'hébergement du Titulaire répond en tout point aux exigences du décret n° 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel.

Une attention particulière sera notamment portée par l'AFLD aux conditions sécurisées d'hébergement, de cloisonnement et de confidentialité de ses données, ainsi qu'aux conditions de continuité d'activité prévues par le titulaire.

L'AFLD exige ainsi un niveau de certification sur les domaines suivants :

- ISO27001 – Mise en œuvre d'un Plan d'Action Sécurisé (PAS) conforme ANSSI
- HDS – Certification pour l'hébergement et l'infogérance des données de santé ;
- RGPD – Validation de la conformité sur la protection des données personnelles.

La politique de sécurité du SI de l'infogérant prestataire doit être conforme à la norme ISO 27002 :2013 qui propose des recommandations en matière de normes organisationnelles relatives à la sécurité de l'information ainsi que des bonnes pratiques de management de la sécurité.

Localisation des données

Les lieux d'hébergement des données doivent satisfaire aux exigences de sécurité de l'AFLD et aux dispositions de la loi du 6 janvier 1978 modifiée, relative à la protection des données personnelles ainsi qu'aux exigences légales en matière de données personnelles de santé. L'AFLD exige que les data-centers hébergeant les données de l'AFLD soient situés au sein de l'UE (union européenne) et de préférence en France.

Maintenance et administration sécurisées du SI AFLD

Le titulaire du présent marché s'assure de respecter les exigences minimales publiées par l'ANSSI concernant les règles d'administration sécurisées du SI AFLD

https://cyber.gouv.fr/sites/default/files/document/ANSSI_PAMS_referentiel_v1.1_vFR.pdf

Le titulaire doit communiquer dans son dossier technique la liste de tous les lieux de stockage de données (site d'hébergement principal, site(s) de secours, etc).

Cloisonnement et isolation par rapport aux infra des autres clients du titulaire

Le titulaire doit assurer l'isolation des données stockées et manipulées ainsi que celle des ressources informatiques mises à disposition de l'AFLD par rapport à celles allouées à ses autres clients, par tout moyen logiciel ou matériel qu'il estime nécessaire.

Le titulaire fourni dans son offre une description du niveau d'isolation proposé et des moyens entrepris. Le titulaire explique les modalités d'assurance de ces différents niveaux de cloisonnement, pouvant aller de l'isolation logique jusqu'à une isolation physique complète. Les impacts de ce cloisonnement sont précisés dans le document technique de l'offre.

Correctifs de sécurité et mises à jour des systèmes

Le titulaire **assure constamment la mise à jour** des systèmes d'exploitation et l'installation des correctifs de sécurité sur les plateformes et systèmes sous sa responsabilité. Les mises à jour concernent les périmètres ci-dessous :

- La plate-forme de virtualisation (le titulaire a l'obligation d'informer l'AFLD de chaque opération majeure sur la plate-forme).
- Les templates (catalogue des OS et images disponibles) de VM. Le titulaire doit mettre à disposition un dépôt local permettant la mise à jour des OS et composants logiciels sans passer par l'accès Internet.
- Tous les serveurs exploités par le titulaire doivent être patchés très régulièrement, en particulier concernant les serveurs exposés sur Internet.

Les serveurs dont la gestion n'est pas confiée au titulaire sont exploités par l'AFLD.

De nouvelles failles sont régulièrement découvertes au cœur des systèmes et logiciels. Ces dernières sont autant de portes d'accès qu'un attaquant peut exploiter pour réussir son intrusion dans le système d'information. Il est donc primordial de s'informer de l'apparition de nouvelles vulnérabilités (CERTFR) et d'appliquer les correctifs de sécurité sur l'ensemble des composants du système **dans un délai d'un mois maximum suivant leur publication par l'éditeur**. La politique de mise à jour du titulaire doit ainsi être définie et déclinée en procédures opérationnelles. Les patchs de mise à jour de niveau CRITIQUE des OS Windows et LINUX doivent être appliqués également dans le mois qui suit la publication par l'éditeur.

3.2.10 Schéma simplifié, organisation hébergement versus infogérance

L'hébergement du système informatique de l'AFLD représente l'externalisation de l'infrastructure matérielle, de sa gestion y compris celle du réseau et des liens de communication nécessaire aux flux d'information entre les data centers et l'Agence. L'hébergeur est donc responsable des serveurs fournis (matériels et virtuels, de la puissance de calcul, de la RAM, de l'espace de stockage, des dispositifs de sécurité, des accès nomades, de tous les liens réseaux de communication).

L'infogérant, responsable de son périmètre, se charge de la gestion quotidienne et du maintien en condition opérationnelle des dispositifs logiciels reposant sur l'infrastructure informatique.

A titre d'illustration, le schéma suivant décrit certaines tâches relevant de l'infogérance et d'autres relevant de l'hébergeur. Cette liste n'est pas exhaustive et a seulement pour objectif de clarifier la frontière entre les prestations décrites ci-après dans le présent cahier des clauses particulières.

Description d'une action	Réalisée par l'hébergeur	Réalisée par l'infogérant
Création d'une machine virtuelle, installation d'un OS, attribution des paramètres demandés (RAM, CPU, disk..)	X	
Supervision de la machine, mise en place des alertes sur les capacités de la VM...	X	
Application de patchs de sécurité sur un logiciel central installé sur une machine hébergée ex.: AD, ou un Exchange, ou un OS		X
Accompagnement dans l'installation d'un progiciel métier ou spécifique en lien avec l'éditeur métier concerné.		X
Réalisation d'une migration d'un applicatif logiciel vers une version majeure		X
Mise en œuvre des sauvegardes des VMs selon la politique définie	X	

4 LOT 1 – Prestation de services pour l’infogérance du système informatique de l’AFLD

4.1 Mise en place / Phase de cadrage : prestation forfaitaire F01 (réversibilité entrante)

Le marché d’infogérance en vigueur sur la période 2021-2025 **arrive à échéance début août 2025**.

Le titulaire de ce lot assure au titre de la prestation de réversibilité (F01) la mise en œuvre de toutes les actions nécessaires à la mise en place l’infogérance proprement dite au niveau opérationnel dans les meilleures conditions de qualité de service et d’efficacité.

Cette période de mise en place est **d’une durée de 3 mois maximum** à compter de la date de notification du marché.

L’AFLD met à la disposition du titulaire la documentation et les éléments en sa possession lui permettant d’appréhender le contexte.

4.1.1 Transfert des prestations

A partir de la situation existante, le titulaire détermine les conditions de transfert des prestations de l’infogérant antérieur vers le titulaire, de telle sorte que les prestations basculent sous son entière responsabilité sans que son intervention puisse être à l’origine d’une interruption des services ou d’une dégradation de la qualité des services produits par l’organisation infogérante précédente.

L’infogérant antérieur de l’AFLD était contractuellement engagé sur les points suivants :

- Transfert des documents
 - Dans le cadre d’un changement de prestataire, il s’est engagé à fournir à l’AFLD tous les documents et procédures nécessaires à la prise en main de la mission d’infogérance actuelle.
 - Transfert de compétences
 - Il s’est engagé, pendant la période de transfert de compétence, à dialoguer avec le titulaire et à lui fournir tous les éléments nécessaires à la poursuite de la mission.
 - Transfert des connaissances
 - Afin d’encadrer le transfert des connaissances et sous la responsabilité de l’AFLD vers le titulaire, il est tenu de répondre à toute demande liée à la poursuite de la mission.
- ⬅ Si l’AFLD valide une insatisfaction des transmissions des informations, elle pourra décider de prolonger la prestation de transfert de connaissances pour une durée égale à 1 mois.

4.1.2 Note de cadrage & réunion de lancement, PAQ, et PAS

A cours de cette phase, le titulaire a en charge la rédaction de la note de cadrage, du plan d’assurance qualité (PAQ), du plan d’assurance sécurité (PAS, voir plus bas). Il a également la charge l’organisation **d’une réunion de lancement** avec les différentes parties du projet.

La note de cadrage a pour objectif d'affiner les exigences du présent cahier des charges en précisant les moyens et la méthode mis en œuvre par le titulaire pour y répondre. Ce document a valeur contractuelle. En annexe de ce document est inclus le PAQ.

Une réunion de lancement est organisée par le titulaire dans un délai de sept (7) jours à compter de la notification du marché afin d'établir le chronogramme des actions à tenir pour prendre en charge l'infogérance. Ce document explique les phases opérationnelles et contient le tableau de bord de suivi opérationnel tout au long de cette mise en place. Il pourra évoluer en fonction des échanges et des décisions entre les parties.

Livrables :

- **Document opérationnel et tableau de bord de suivi issus de la réunion de lancement**
Délai : T0 + 10 jours
- **Note de cadrage et du PAQ**
Délai de livraison : T0 + 1 mois = T1
La validation de la note de cadrage et du PAQ a lieu au plus tard à T0 + 3 mois
- **Plan d'assurance sécurité (PAS)**
Délai : T0 + 3 mois

T0 est la date de notification du marché. Le cas échéant, les délais d'exécution mentionnés ci-dessus seront prolongés d'une durée égale à l'éventuelle prolongation de la phase de transfert de compétences.

L'élaboration de ces documents se fait dans le cadre d'un dialogue constant avec l'AFLD. La validation de la note de cadrage (et ses annexes) déclenche l'exécution des prestations de la phase opérationnelle de l'infogérance.

T1 est la date de validation de la note de cadrage (et du PAQ) et correspond à la date de démarrage de la phase opérationnelle d'infogérance.

4.2 Infogérance en mode opérationnel – prestation forfaitaire F02

Les prestations suivantes forment la base de la prestation d'infogérance F02 dans le périmètre spécifié infra :

- Maîtrise d'œuvre de l'infogérance et pilotage,
- Support aux utilisateurs
- Administration et l'exploitation des systèmes,
- Gestion de la messagerie électronique,
- Gestion des changements informatiques.

4.2.1 Périmètre de départ de l'infogérance, systèmes du SI AFLD

Lors de la mise en place de l'infogérance, le titulaire prend donc en charge le maintien en condition opérationnelle des dispositifs suivants.

Hyperviseur	Machine Virtuelle	En Cluster	vLAN	fonction	OS
POOL infogéreur	AD-1	Oui	1	Contrôleur de domaine, AD, DHCP, DNS	Win Standard supporté, à jour
POOL infogéreur	AD-2	Oui	1	Contrôleur de domaine, AD, DHCP, DNS	Win Standard supporté, à jour
POOL infogéreur	RH-1	Non	1	Plateforme de gestion des congés et de paie legacy	Win Standard supporté, à jour
Pool infogéreur	WPAIE-1	Non		Plateforme de gestion de la paie	Win Standard supporté, à jour
POOL infogéreur	CHORUS	Non		Interface serveur GBCP et plateforme externe CHORUS	CentOS
POOL infogéreur	GBCP	Non		Serveur de gestion comptable et budgétaire	Win Standard supporté, à jour
POOL infogéreur	DATAS	Non		Serveur de fichiers AFLD	Win Standard supporté, à jour
POOL infogéreur	EXCH	Non		Serveur de messagerie exchange, BAL & transport	Win Standard supporté, à jour
POOL infogéreur	GED-1	Non		Serveur gestion qualité	Win Standard supporté, à jour
POOL infogéreur	NPS-1	Non		Serveur Radius Paris Authentification racine	Win Standard supporté, à jour
POOL infogéreur	SECU-1	Non		Serveur de gestion du parc SI afd	Win Standard supporté, à jour
POOL infogéreur	SECU-2	Non		Appliance dédiée pour solution antiviral des postes clients AFLD	Ubuntu
Pool infogéreur	AUT-PP	Non		Serveur applicatif	Debian GNU/Linux
Pool infogéreur	MAGP-1	Non		Serveur applicatif	Debian GNU/Linux
Pool infogéreur	MAGPDB -1	Non		Serveur applicatif	Debian GNU/Linux
Pool infogéreur	MAGPP-1	Non		Serveur de pre production applicatif	Debian GNU/Linux
Pool infogéreur	PP-GED-1	Non		Serveur de preproduction applicatif	Win Standard supporté, à jour
Pool infogéreur réduit (supervision seule)	hvp01	Non		Hyperviseur local sur site PARIS	Win Standard supporté, à jour
Pool infogéreur réduit (supervision seule)	imp01	Non		VM serveur d'impression local PARIS	Win Standard supporté, à jour
Pool infogéreur réduit (supervision seule)	wds01	Non		VM serveur de mise à jour local PARIS	Win Standard supporté, à jour
Pool infogéreur réduit (supervision seule)	Dispositifs commutateurs	Non		Paris ARUBA (6 dispositifs)	

Ce descriptif reflète la situation au moment de l'écriture du cahier des charges. Il sera repris et éventuellement amendé au moment de l'installation du titulaire.

4.2.2 Support aux utilisateurs – Prestation forfaitaire F03

4.2.2.1 Prestations attendues du support de niveau 2 et 3 et son périmètre

Le support aux utilisateurs de niveau 1 est assuré par l'équipe interne SI de l'AFLD.

L'équipe SI AFLD demande au titulaire de prendre en charge le support de niveau 2 (ou 3) du système d'information de l'AFLD dans le périmètre qui est le sien. Seuls les membres de l'équipe SI de l'Agence peuvent contacter l'infogérant. Il n'y a pas de contact direct entre l'infogérant et les agents AFLD (autre que ceux du SI).

Les demandes remontées par AFLD doivent de ce fait suivre un traitement particulier sans perte de temps par le passage N1 mais être immédiatement prises en charge par les équipes de niveau 2 et 3.

La définition classique des niveaux de support informatique est rappelée ci-après :

Niveau 1	Le technicien de niveau 1 prend en charge la demande d'assistance, l'enregistre dans une base de données, diagnostique le problème et donne des conseils de base pour sa résolution. Il peut résoudre les problèmes les plus courants rencontrés par les utilisateurs et peut s'aider d'une base de connaissances interne au besoin. Si la démarche n'aboutit pas (niveau de compétence, problèmes plus pointus, etc.), il passe le relais à un intervenant de niveau 2.
Niveau 2	L'intervenant de niveau 2 peut diagnostiquer la panne (si le niveau 1 ne l'a pas déjà fait), faire rentrer le matériel en atelier ou déclencher une intervention sur site. Il est à même de guider l'utilisateur par téléphone pour la résolution complexe du problème. Selon les systèmes il peut être amené à prendre le contrôle à distance (s'il dispose des autorisations nécessaires).
Niveau 3	Ce niveau est le prolongement du niveau 2 pris en charge par un spécialiste du problème de référence, et peut être en lien avec un autre expert externe (fournisseur, éditeur de logiciels, constructeur informatique, etc.).

Source ITIL

Les demandes reçues par le titulaire concernent aussi bien les demandes de résolution d'incidents que des demandes de travaux d'exploitation ponctuels (restauration d'archives par exemple), des demandes d'intervention à planifier (installation, évolution logicielle ou matérielle...) ou encore des demandes d'informations ayant trait aux systèmes informatiques du périmètre d'exercice des prestations.

Le titulaire assure la prise en charge des incidents mettant en jeu un tiers avec lequel l'AFLD a un contrat (hébergeur, opérateurs de réseaux, fournisseur d'équipement utilisateurs, fournisseurs équipements réseaux). A ce titre, il facilite ou assure la déclaration de l'incident auprès du tiers correspondant, veille à son traitement, à la validation et à la livraison de la correction éventuelle effectuée par le tiers avant sa clôture définitive.

Comme décrit dans le paragraphe 4.2.1.9 traitant du reporting, le titulaire tient à jour un tableau de bord récapitulatif des incidents traités : description de l'incident, zone impactée, nom de l'utilisateur concerné, date et heure d'ouverture et de clôture de l'incident, moyens mis en œuvre, contournement utilisé le cas échéant, correction apportée etc...

Ainsi, les prestations essentielles du support utilisateur sont de :

- Constituer un point unique de collecte, de coordination et de diffusion de l'information,
- Tenter de résoudre les incidents par téléphone ou prise en main à distance, ou déplacements,
- Enregistrer, instruire et suivre les dossiers jusqu'à leur clôture,
- Relancer les intervenants quels qu'ils soient, si nécessaire,
- Informer le SI AFLD de façon préventive en cas de connaissance de circonstances génératrices de dysfonctionnements (potentiels ou pas),
- Alimenter les indicateurs d'activité et de niveau de service.

4.2.2.2 Traitement des demandes, résolution des incidents

Le titulaire présente sa procédure de gestion des incidents en phase de cadrage. Cette procédure décrit les étapes classiques suivantes :

Accueil de la demande > qualification, classification > traitement > résolution et clôture

Les procédures d'escalade et de gestion des priorités sont également décrites.

Le titulaire met en œuvre ces procédures validées par l'AFLD pour répondre aux sollicitations des utilisateurs.

A minima, le titulaire respecte les conditions suivantes :

Chaque demande doit être identifiée par un numéro unique, un libellé, une description longue, un statut (ouvert, en cours, fermé), une catégorie (question, changement, dysfonctionnement), une priorité (sans objet, mineure, majeure, bloquante).

Chaque incident doit être pris en charge **dans l'heure** (en HSN) après la demande de l'équipe SI interne.

Chaque dysfonctionnement doit être traité (résolu ou à minima un contournement est proposé) selon les délais :

Priorité établie du dysfonctionnement	Délai attendu de résolution (HSN)**
Mineure	4 heures
Majeure	3 heures
Bloquant*	1 heure

(*) Bloquant signifie que le service considéré est totalement indisponible en production

(**) Le titulaire n'est responsable que de la partie du processus qui lui incombe. Si le titulaire, lors de la résolution d'un incident, doit s'appuyer sur un tiers pour pouvoir le résoudre (exemple : incident réseau Wan) le temps pris par le tiers pour résoudre le problème sera déduit du temps de traitement par le titulaire.

4.2.2.3 Accessibilité du support infogérant

Le SI AFLD a plusieurs moyens, mis en place par le titulaire, d'accéder au support informatique

- **Le numéro direct du contact technique** du compte (ROC, voir chapitre correspondant) [utilisé uniquement par le RSI AFLD]**
- par un numéro de téléphone unique (non surtaxé) vers le centre de support**
- par messagerie électronique (BAL) vers le centre de support 24h/24 7j/7
- par une plateforme intranet dédiée* accessible 24h/24 7j/7

*Dans tous les cas, la demande formulée fait l'objet d'une entrée dans la plateforme intranet, outil de gestion des incidents/interventions du titulaire ; un courriel standard est envoyé au demandeur précisant la prise en compte de la demande et le numéro de ticket.

Cet outil permet aussi à la MOA informatique de l'AFLD de visualiser (en temps réel) le suivi des différentes demandes (en cours ou fermées) et de disposer d'un premier niveau de statistiques de suivi.

**dans les heures de service normal comme précisé dans le chapitre 8

Plus globalement, un outil web est mis à disposition du responsable SI AFLD afin de visualiser/analyser/reporter toutes actions opérées par le titulaire (actions de support utilisateur jusqu'aux actions de MCO de l'infrastructure)

L'outil expose un certain nombre de champs (type d'intervention, zone fonctionnelle, degré d'urgence ou de criticité). Le titulaire renseigne chaque cas de la manière la plus précise possible, en le requalifiant au besoin. Il est responsable de la mise à jour régulière des champs de chaque incident jusqu'à la clôture de celui-ci.

4.2.3 Maîtrise d'œuvre et pilotage de l'infogérance – prestation forfaitaire F04

Les services attendus au titre du pilotage sont :

- L'élaboration, l'analyse et la communication à l'AFLD des éléments de pilotage. Le pilotage s'adosse à des tableaux de bords standards et élaborés mensuellement par le titulaire. Ils constituent le socle des échanges en comité et s'appuient sur des éléments factuels (outillage, log, etc.),
- Le pilotage des incidents en fonction de leur sévérité,
- Le contrôle qualité de la prestation (contrôle du respect du PAQ, du PAS, contrôle de la validité des référentiels documentaires et techniques, contrôle de la qualité des indicateurs, etc.),
- Le maintien à jour de la documentation Qualité (PAQ, PAS), du plan et du référentiel documentaire de réversibilité,
- L'identification et le suivi des risques,
- Le conseil et le suivi d'amélioration continue

4.2.3.1 Pilotage de l'infogérance, SDM, ROC : interlocuteurs exigés dans le cadre de la prestation

Le titulaire assure un rôle de direction et de coordination couvrant l'ensemble des prestations qui lui sont confiées.

Tout au long de la prestation, l'AFLD exige d'être en lien constant avec le titulaire et de bénéficier du dialogue régulier avec deux profils bien identifiés :

Le Titulaire désigne **un interlocuteur technique pour l'AFLD (ROC)** dont la mission principale est le pilotage et la coordination technique des prestations. Il :

- Possède une connaissance détaillée de l'environnement technique AFLD
Veille au respect des règles de sécurité ;
- Assure la coordination technique de l'ensemble des prestations ;
- Propose des plans d'amélioration ou d'actions correctives ;
Propose des améliorations techniques, des solutions et prend en compte les problématiques métiers de l'AFLD et ses exigences de sécurité
- A autorité pour prendre toutes les décisions opérationnelles courantes et urgentes.

C'est le référent technique de l'AFLD.

Il est présent lors des comités techniques réguliers.

Le titulaire désigne **un interlocuteur principal pour le contrat (SDM)** dont la mission principale est la coordination de l'ensemble des prestations fournies et le contrôle de la qualité de service. Il :

- Prend en charge le suivi administratif et financier du marché ;
- Est garant du respect des engagements et de la qualité de service ;
- Veille au respect des règles de sécurité ;
- Assure la coordination de l'ensemble des prestations ;
- Veille à la qualité opérationnelle du service ;
- Met en œuvre les moyens, garantit leur permanence, les adapte afin de respecter les engagements contractuels ;

Il est présent lors des comités techniques réguliers.

Le Titulaire désigne **un interlocuteur RSSI** dont la mission principale est d'intervenir sur tous les sujets liés à la sécurité du SI. Il :

- Est le RSSI référent au sein de l'entité du titulaire
Veille au respect des règles de sécurité ;
- Répond aux questions spécifiques sur la sécurité du SI que AFLD pourrait avoir au cours du marché (parfois en lien avec l'ANSSI) ;
- Propose des plans d'amélioration, des améliorations techniques ou des actions correctives dans ce domaine ;
- A autorité pour prendre toutes les décisions opérationnelles courantes et urgentes.

Il est présent selon le besoin lors des différents comités ou réunions spéciales traitant de la sécurité.

Le RSI et le responsable technique SI de l'AFLD sont les interlocuteurs principaux de l'Agence et ont autorité pour prendre les décisions courantes ou urgentes.

4.2.3.2 Devoir d'alerte, de conseil

Le titulaire est tenu à une obligation générale de conseil, d'information et de recommandation, et de mise en garde, sur le périmètre contractuel.

Ce rôle peut être tenu particulièrement par le responsable opérationnel du compte pour l'Agence.

Le devoir de conseil et d'alerte auprès d'AFLD contribue à l'amélioration de la performance du service et à la réduction des coûts des services associés. Le titulaire s'engage à émettre auprès d'AFLD tous les conseils et mises en garde nécessaires au cours de l'exécution du marché notamment en termes de qualité de service, de continuité d'exploitation, **de sécurité et de mise à l'état de l'art et d'évolution**.

Il propose toute adaptation, amélioration, modernisation ou mise à niveau du SI qu'il juge souhaitable en vue d'optimiser les performances et les coûts de fonctionnement. Ceci s'applique aussi bien aux aspects techniques que méthodologiques ou organisationnels et s'appuie notamment sur l'analyse des indicateurs, la prise en compte des remontées clients et sur une gestion des problèmes (au sens ITIL du terme) permettant d'identifier les incidents récurrents afin de traiter les causes plutôt que les symptômes.

Dans le cadre de son obligation de conseil, le titulaire informe AFLD dès qu'il a connaissance de toute nouveauté technologique, ou nouveau produit ou service, plus adapté aux besoins d'AFLD en termes de coûts, de qualité des services ou de maîtrise des risques.

L'apport de conseil porte au minimum sur :

- Les technologies : tendances, opportunités, caractéristiques, valeur ajoutée, etc.,
- Les nouvelles versions et/ou les versions en place qui ne sont ou ne seront plus supportées,
- L'amélioration de l'organisation et de la coordination,
- Les opportunités de réduction de coûts,
- Les opportunités d'amélioration de la qualité des services,
- La sécurité du SI

La veille technologique est assurée par le Titulaire. Il est attendu de ce dernier un apport important sur ces champs compte tenu de son expérience, de sa visibilité sur les contrats clients, et de ses capacités de mutualisation des moyens.

A minima, le titulaire préconise **deux actions d'amélioration par an**. Ces dernières seront examinées en Comité de Pilotage, et éventuellement présentées en Comité Stratégique pour arbitrage et validation.

- L'AFLD se réserve le droit de suite quant aux évolutions et/ou améliorations proposées par le titulaire.

4.2.3.3 Plan d'Assurance Qualité

Le titulaire a la responsabilité de l'élaboration et de la mise à jour du PAQ qui recense l'ensemble des prestations.

La liste suivante est une liste non exhaustive des points qui sont mentionnés dans le PAQ :

- Les interlocuteurs des parties
- Le fonctionnement du comité de pilotage technique
- Le fonctionnement ces cellules de crises
- Le reporting : tableaux de bord, indicateurs
- Les procédures d'incitation au maintien de la qualité
- Les normes de présentation des documents

- La documentation de l'architecture du système d'information
- La classification des applications par niveau de criticité
- Les processus et délais d'administration et d'exploitation
- Les processus et les délais d'alerte
- Les processus de gestion des incidents et des processus d'escalade
- Les processus de gestion des sauvegardes informatiques
- Les processus de demande de service exceptionnels
- Les processus et délais de demande, d'exécution, de recette des installations
- Les processus et délais de demande de changements,
- Les règles et processus de sécurité
- Les règles et les processus de réversibilité
- Les processus d'utilisation de l'outil de suivi du support

4.2.3.4 Plan d'assurance sécurité – PAS

Le titulaire élabore le plan d'assurance sécurité qui formalise précisément tous les dispositifs qu'il s'engage à mettre en œuvre pour répondre aux exigences de sécurité et de gestion des risques opérationnels sur le périmètre infogéré du système d'information de l'AFLD.

4.2.3.5 Comités

Le titulaire organise plusieurs réunions, notamment au début du marché. Parmi celles-ci figurent à minima :

- La réunion de lancement
- La réunion de fin de cadrage (T1)
- Un comité de suivi technique et opérationnel **mensuel**, qui traite les priorités, les échanges techniques, l'information utile, le planning à court et moyen terme. Les interlocuteurs sont à minima le SDM, le ROC. **La présence du référent technique (ROC) est impérative** lors des COTECH.
- Des COPIL, à fréquence **trimestrielle durant toute la période d'exécution du marché**. Les interlocuteurs sont à minima le SDM, un responsable de niveau décideur* et le responsable commercial du compte. **La présence du responsable 'décideur' est impérative** lors des COPIL
- Un comité « innovation & évolutions » / stratégie **annuel** est organisé avec les parties

*Lors des COPIL, l'AFLD est représentée par son **Secrétaire Général adjoint**, membre du comité de direction de l'Agence. Un membre de niveau direction représente le titulaire lors de ces comités de pilotage.

Le compte-rendu des différentes réunions est transmis par le titulaire à l'AFLD dans un délai de 5 jours ouvrés maximum à compter du lendemain de la réunion. L'AFLD dispose d'un délai de 5 jours ouvrés à compter de la réception du compte-rendu pour approuver ou émettre d'éventuelles réserves auquel cas une nouvelle version sera émise par le titulaire, l'objectif étant de finaliser le compte rendu dans les 10 jours suivants la réunion.

4.2.3.6 Comité technique

Le Comité technique (COTECH) est la réunion opérationnelle et technique. Il se réunit de façon mensuelle (sur le site de l'AFLD ou en visio ou audio conférence).

Sans que cette liste soit limitative, il :

- Suit l'avancement des projets en cours,
- Traite les points bloquants du moment, examine les solutions, échange les conseils,
- Donne les indicateurs techniques (consommation des volumes, puissance utilisée...),
- Relève/anticipe les avertissements/alertes,
- Emet des préconisations techniques,
- Décide des traitements techniques,
- Etabli un plan d'actions techniques,
- Donne une synthèse de l'activité passée sur le mois,
- Décide des remontées vers le COPIL le cas échéant,

Le compte-rendu des différentes réunions est transmis par le titulaire à l'AFLD dans un délai de 5 jours ouvrés maximum à compter du lendemain de la réunion. L'AFLD dispose d'un délai de 5 jours ouvrés à compter de la réception du compte-rendu pour approuver ou émettre d'éventuelles réserves auquel cas une nouvelle version sera émise par le titulaire, l'objectif étant de finaliser le compte rendu dans les 10 jours suivants la réunion.

Ce comité est animé par le titulaire (ROC). Le responsable technique de l'AFLD est présent.

4.2.3.7 Comité de pilotage

Le Comité de Pilotage est l'instance de pilotage contractuelle et décisionnelle. Il se réunit de façon trimestrielle (sur le site de l'AFLD ou en visio ou audio conférence).

Sans que cette liste soit limitative, il :

- Contrôle la qualité des prestations effectuées par le titulaire, expose les indicateurs pertinents de suivi de la prestation
- Décide de plans d'améliorations,
- Suit l'avancement des projets,
- Préconise des évolutions de périmètre et des services,
- Décide de l'application et du quantum des pénalités appliquées,
- Prépare les orientations et les évolutions du Système d'Information de l'AFLD,
- Assure le suivi financier du contrat,
- Assure le suivi des documents contractuels révisables,
- Prépare l'ordre du jour des Comités Stratégiques.

Le compte-rendu des différentes réunions est transmis par le titulaire à l'AFLD dans un délai de 5 jours ouvrés maximum à compter du lendemain de la réunion. L'AFLD dispose d'un délai de 5 jours ouvrés à compter de la réception du compte-rendu pour approuver ou émettre d'éventuelles réserves auquel cas une nouvelle version sera émise par le titulaire, l'objectif étant de finaliser le compte rendu dans les 10 jours suivants la réunion.

En cas de points de vue opposés et non conciliables, le différend est acté dans le compte-rendu et soumis au Comité Stratégique.

L'ordre du jour des Comités de Pilotage intégrera notamment les éléments suivants :

- Les faits marquants de la période ;
- Une analyse commentée par le titulaire des tableaux de bord mensuels comprenant les indicateurs, les éléments de volumétrie, les éléments de sécurité ;
- Une revue des principaux changements et des mises en production du mois écoulé, ainsi que des prévisions à 3 mois ;
- Une revue d'avancement des projets ou études en cours (jalons, dates impératives, ...) ;
- Une revue des risques ;
- Un suivi des préconisations issues des rapports incidents techniques et de leur mise en œuvre en comité opérationnel ;
- Une fois par an, une vérification du Plan de réversibilité et du Plan d'Assurance Qualité (PAQ)
- Deux fois par an, une vérification du Plan d'Assurance Sécurité (PAS), du référentiel documentaire de réversibilité ;
- Validation des plannings.

Le Comité de pilotage est composé notamment de représentants de chacune des parties ayant des responsabilités leur permettant d'assumer les fonctions de décision et le contrôle de l'exécution du marché.

Ce comité est animé par le représentant de la direction générale du titulaire. L'ordre du jour et le document support à la réunion sont proposés par le titulaire à l'AFLD au plus tard 5 jours ouvrés avant la réunion, l'AFLD pouvant faire des remarques au plus tard la veille de cette réunion.

4.2.3.8 Comité Innovations et Evolutions

Le Comité Innovation et Evolutions se réunit pour permettre aux parties d'échanger sur les innovations et évolutions planifiées ou prévisibles en matière de système d'information. C'est aussi l'occasion de discuter des feuilles de route à moyen et long terme des entités.

Plus spécifiquement, et sans que cette liste soit limitative, il :

- Revisite et valide (le cas échéant) les changements importants proposés par le Comité de Pilotage ;
- Acte de certaines évolutions du périmètre des prestations ;
- Étudie et propose des avenants au marché ;
- Effectue une revue des évolutions du SI AFLD et du plan industriel du titulaire pouvant avoir des incidences sur le déroulement du marché ;
- Permet l'échange des informations stratégiques des deux parties.
- Reprend la cartographie applicative du SI et exprime les innovations et évolutions pouvant être étudiées pour l'amélioration de la performance du système

Le compte-rendu des différentes réunions est transmis par le titulaire à l'AFLD dans un délai de 5 jours ouvrés maximum à compter du lendemain de la réunion. L'AFLD dispose d'un délai de 5 jours ouvrés à compter de la réception du compte-rendu pour approuver ou émettre d'éventuelles réserves auquel cas une nouvelle version sera émise par le titulaire, l'objectif étant de finaliser le compte rendu dans les 10 jours suivants la réunion.

Ce comité est co-animé par le représentant de la direction générale du titulaire et par le secrétaire général ou son représentant de l'AFLD. L'ordre du jour et le document support à la réunion sont proposés par le titulaire à l'AFLD au plus tard 5 jours ouvrés avant la réunion, l'AFLD pouvant faire des remarques au plus tard la veille de cette réunion.

4.2.3.9 Documentation, mise à jour constante

Le titulaire doit fournir à l'AFLD, chaque année (date d'anniversaire de la prestation + 1 mois maximum), les versions mises à jour des documents suivants :

- Plan d'assurance qualité
- Plan d'assurance sécurité
- Plan de réversibilité

4.2.4 L'administration et l'exploitation des systèmes

L'exploitation des systèmes est l'ensemble des activités récurrentes assurant le fonctionnement des systèmes informatiques en environnement de production ; l'administration des systèmes est l'ensemble des activités récurrentes contribuant à maintenir opérationnel l'environnement d'exploitation.

4.2.4.1 Généralités

Le titulaire mesure et maintient la qualité de service attendue. Les attentes de l'AFLD en matière de qualité de service sont précisées au chapitre traitant de la convention des services.

Les activités récurrentes couvrent au minimum les fonctions suivantes :

- Gestion des configurations des systèmes [Operating System, console antivirus pour les serveurs et systèmes hébergés]
- Gestion des comptes utilisateurs, fonctionnels, administrateurs ou de service de l'annuaire AD de l'Agence selon les besoins (mouvements de personnels, fonctionnement applicatifs métiers, etc.)
- Gestion de l'Active directory et de ses services annexes (GPO, groupes AD, journaux d'évènements, NTP, scripts, etc...)
- Gestion des serveurs DNS internes
- Mise à niveau des logiciels (patchs critiques)
- Gestion des serveurs d'impression (ajout d'imprimante...)
- Assistance du service informatique dans le cadre de la réception et la mise en production de nouvelles solutions / version applicatives
- Pilotage des serveurs
- Gestion des incidents d'exploitation (ex. : anomalies exchange...)
- Applications des procédures prévues en matière de sécurité
- Réalisation d'opérations courantes
- Gestion des alarmes de supervision

4.2.4.2 Description des prestations

Administrations des systèmes

- Gestion des configurations : assurer le fonctionnement et l'évolution des systèmes
 - Planifier et exécuter les arrêts des systèmes pour la maintenance périodique,
 - Planifier et piloter les modifications de configurations,
 - Actualiser la documentation,
 - Assurer le support N2, N3
- Mise à niveau des logiciels de base :
 - Planifier et effectuer les mises à jour (petites évolutions, nouvelles versions, correctifs) des logiciels des systèmes d'exploitation, des SGBD le cas échéant, des outils d'exploitation...,
 - Contrôler les logiciels installés en termes d'environnement, de version, de License.
 - Gestion des performances : maintenir des performances optimales au cours du temps
 - Préconiser les évolutions souhaitables de configuration.
- Surveillance et optimisation technique des bases de données :
 - Le titulaire assure les opérations simples d'administration des bases de données (arrêt/redémarrage du serveur, backup, restauration des données). L'AFLD dispose aujourd'hui de bases de données de type relationnelles SQLServer, PostGresql (non exhaustif),
- Gestion des sécurités :
 - Conseiller la MOA sur la gestion de la sécurité des applications, accès et modifications des sources, gestion des habilitations,
 - Conseiller pour la mise en œuvre les règles de gestion des mots de passe et des droits d'accès,

Exploitation des systèmes

- Pilotage des serveurs :
 - Arrêter et relancer les serveurs, les systèmes, les logiciels de base, les bases de données...
 - Arrêter, relancer les applications, selon les procédures d'arrêt/redémarrage correspondantes à l'application,
 - Prendre toute mesure préventive de nature à éviter tout blocage d'un serveur,
- Gestion des incidents d'exploitation :
 - Enregistrer les incidents d'exploitation et effectuer un premier diagnostic,
 - Faire les demandes d'intervention nécessaires selon le besoin aux services de l'hébergement de l'infrastructure (augmentation de capacité, espace disque...),
 - Transmettre à la MOA SI AFLD les demandes d'intervention nécessaires selon le besoin vers les services tiers de supports applicatifs (ex : support Gandi, support Telephonie,...),
 - Assurer les interventions nécessaires, mettre en place un contournement de l'incident, corriger l'incident,
 - Documenter les incidents,

- Alimenter le tableau de bord mensuel de reporting.

4.2.5 La gestion de la messagerie électronique

Les prestations mises à la charge du titulaire pour la gestion de la messagerie concernent les opérations suivantes :

- Assistance pour les opérations liées aux adresses (création modification, suppression), aux listes de diffusion, aux calendriers partagés, aux dossiers publics...
- La mise à jour du logiciel, l'installation des patchs de sécurité
- Le cas échéant, la gestion, l'administration des comptes utilisateurs sur la plateforme antispam de l'AFLD
- Le cas échéant, la mise en place et le maintien en condition opérationnelle de la sauvegarde des logs transactionnelles d'échange (IIS, suivi des messages)
- La gestion du serveur Exchange et de ses services annexes (Banques de données, BAL, ressources partagées, droits d'accès, IIS, etc...),
- Les paramétrages de sécurité,
- La gestion du certificat Exchange,
- La surveillance des services,

4.2.6 La gestion des changements informatiques

On appelle changement toute opération non récurrente qui s'avère nécessaire pour maintenir le SI opérationnel en respectant les engagements sur les niveaux de services précisés au paragraphe 6.

Tout changement nécessite un délai de préavis.

Ce délai est la durée entre la transmission au titulaire d'une demande de changement à venir, et la prise d'effet dudit changement avec son intégration dans le périmètre d'exercice des prestations du titulaire.

Les procédures de recette sont décrites dans le PAQ.

4.2.7 Prestations annexes

Les prestations annexes correspondent à des prestations non comprises dans les prestations de base de l'infogérance (prestations à prix global et forfaitaire) décrites supra.

Elles sont déclenchées, si le besoin apparaît, par bon de commande.

Les prestations annexes font l'objet de commandes d'unités d'œuvre décrites et chiffrées dans le cadre de réponse financier.

Elles permettent de répondre à tout projet d'envergure initié par l'AFLD, sur les conseils ou non du titulaire, nécessitant une phase d'étude détaillée et ayant une incidence majeure sur le système d'information de l'AFLD.

Tout projet de ce type donne lieu à une étude préalable réalisée par le titulaire pour évaluer une enveloppe en termes de charge de travail, de délai et de budget.

Le titulaire propose une typologie des intervenants susceptibles d'intervenir pour la mise en œuvre de ces prestations (formateur, chef de projet, technicien, ingénieur).

Au titre de l'obligation de conseil mise à la charge du titulaire au titre du présent marché, cette étude préalable est comprise dans les prestations de base de l'infogérance.

Ces prestations annexes sont à traiter comme des projets à part entière.

- Les prestations annexes portent sur :
 - Le transfert important d'équipements d'un site à un autre (déménagement),
 - La prestation d'assistance et de conseil hors périmètre,
 - Le projet de migration majeure (Active directory, Exchange, ...)
 - Des travaux d'études et de réalisations spécifiques dans le cadre d'une évolution majeure du SI de l'AFLD (mise en place d'un système de haute disponibilité tier, d'une appliance de sécurité...)
- Ne relèvent pas des prestations annexes mais sont comprises dans le périmètre de base de l'infogérance (liste non exhaustive) :
 - Les évolutions normales du SI,
 - L'installation d'une nouvelle application,
 - La réinstallation d'une application existante,
 - Les conseils courants.

5 LOT 2 – Prestation de services pour l'hébergement du système informatique de l'AFLD, services et fournitures des liens de connexions avec le data center

5.1 Périmètre de la prestation d'hébergement et FAI

Le titulaire a défini dans son offre l'architecture technique qu'il met en place pour assurer l'exécution des prestations d'hébergement du système informatique de l'AFLD afin :

- De satisfaire un hébergement assurant les niveaux de sécurités et les normes spécifiés dans le paragraphe 3.2.15 de ce document
- De satisfaire un hébergement de l'infrastructure AFLD telle que décrite dans les paragraphes 3.2.1 à 3.2.5 du document
- De satisfaire un hébergement assurant les niveaux de services spécifiés plus bas dans ce document (& 4.4)
- De satisfaire les capacités de communications définis dans ce document par la mise en place de liens opérateurs [&5.2]
- De satisfaire les exigences d'accès à son SI exprimées par l'AMOA AFLD. [& 5.3]

Le titulaire assure le maintien en condition opérationnelle, l'exploitation, la supervision de tous ces dispositifs.

En tant qu'hébergeur, il fournit également les moyens qui permettront de répondre aux exigences de sauvegarde exprimées dans ce document.

5.1.1 Socle de l'infrastructure de départ

Le titulaire fournit à l'AFLD l'infrastructure pour héberger l'ensemble des dispositifs SI décrits dans les paragraphes 3.2.1 à 3.2.5 et précisés ci-après.

Ce socle peut donc être schématiquement représenté par les x VMs (virtual machines) actuellement utilisées au sein du SI AFLD. A son arrivée, le titulaire réserve un « espace » de puissance informatique. Cet espace, décrit dans le plan de migration du titulaire, sera la destination de toutes les VMs et machines physiques actuelles du SI AFLD.

Le titulaire respectera les caractéristiques minimales de chaque VM / machine qui sont exposées ci-dessous :

Hyperviseur	Machine Virtuelle	vLAN	RAM DISK	vCPU	fonction	OS
POOL infogéreur	AD-1	PROD	8 100	4	Contrôleur de domaine, AD, DHCP, DNS	Win Standard, supporté, à jour
POOL infogéreur	AD-2	PROD	8 100	4	Contrôleur de domaine, AD, DHCP, DNS	Win Standard, supporté, à jour
POOL infogéreur	RH-1	PROD	12 250	4	Plateforme de gestion des congés et de paie legacy	Win Standard, supporté, à jour
Pool infogéreur	WPAIE-1	PROD	6 180	2	Plateforme de gestion de la paie	Win Standard, supporté, à jour
POOL infogéreur	CHORUS	DMZ	4 100	2	Interface serveur GBCP et plateforme externe CHORUS	CentOS Linux release 7.2.1511 (Core)

POOL infogéreur	GBCP	PROD	16 550	4	Serveur de gestion comptable et budgétaire	Win Standard, supporté, à jour
POOL infogéreur	DATAS	PROD	16 1500	4	Serveur de fichiers AFLD	Win Standard, supporté, à jour
POOL infogéreur	EXCH	PROD	24 700	8	Serveur de messagerie exchange, BAL & transport	Win Standard, supporté, à jour
POOL infogéreur	GED-1	PROD	10 540	4	Serveur gestion qualité	Win Standard, supporté, à jour
POOL infogéreur	NPS-1	PROD	4 50	2	Serveur Radius Paris Authentification racine	Win Standard, supporté, à jour
POOL infogéreur	SECU-1	PROD	12 100	4	Serveur de gestion du parc SI afd	Win Standard, supporté, à jour
POOL infogéreur	SECU-2	PROD	15 130	6	Appliance dédiée pour solution antivirus des postes clients AFLD	Ubuntu 20.04.6 LTS
Pool infogéreur	AUT-PP	PROD	4 30	2	Serveur applicatif	Debian GNU/Linux 11 (bullseye)
Pool infogéreur	MAGP-1	DMZ	6 280	2	Serveur applicatif	Debian GNU/Linux 11 (bullseye)
Pool infogéreur	MAGPDB-1	PRODDB	6 80	2	Serveur applicatif	Debian GNU/Linux 11 (bullseye)
Pool infogéreur	MAGPP-1	RECET	10 280	4	Serveur de pre production applicatif	Debian GNU/Linux 11 (bullseye)
Pool infogéreur	PPGED-1	RECET	10 540	4	Serveur de preproduction applicatif	Win Standard, supporté, à jour

Ce descriptif reflète la situation au moment de l'écriture du cahier des charges. Il sera repris et éventuellement amendé au moment de l'installation du titulaire.

Cette liste de VMs représente les fonctions nécessaires centrales et applicatives. Cependant, il existera au sein de l'infra des VMs mises en place par le titulaire et nécessaires pour répondre à des exigences particulières telles que :

- Récupération et historisation des logs et journaux des différents serveurs centraux (AD1 et AD2, Exchange, Parefeu) au sein d'un serveur SYSLOG, permettant de garder l'historique sur 1 année de tous les événements principaux
- Autres systèmes virtuels ou physiques nécessaires pour la supervision, la sécurité ou la sauvegarde, sous la responsabilité du titulaire,
- serveurs pour l'application des mises à jour,
- .../...

Les VMs peuvent reposer sur un ensemble d'hyperviseurs mutualisé par l'hébergeur mais en respectant les conditions d'étanchéité précisées plus haut dans ce document.

5.1.2 Liens de communications (F03 – COMM INSTALL)

Le titulaire met en place les liens de communications suivants :

- Lien principal dédié fibre entre AFLD et le data center de l'hébergeur :
 - o Débit garanti symétrique **minimum** de 500Mbs-1
- L'accès à internet depuis le site AFLD se fera par l'infrastructure du titulaire. Celui-ci mettra en œuvre une sortie pour AFLD de débit minimal 200Mbs-1.
- Un pool minimal **de 10 adresses IPs publiques** sera fourni à l'AFLD.

Les technologies utilisées sont celles spécifiées par le titulaire dans son offre technique. Elles répondent aux exigences exprimées dans les paragraphes 3.2.15. Le titulaire place notamment sur la ligne internet les dispositifs de sécurité et d'optimisation des flux, la capacité de réservation de bande passante à la demande de l'AFLD (QOS).

La ligne fibre est supervisée par le titulaire qui doit être capable d'exposer à l'AFLD l'historique de disponibilité, son débit.

Le titulaire installe les dispositifs (routeurs/parefeu) au sein des locaux techniques de l'AFLD. Ces dispositifs sont maintenus et supervisés par ses soins.

Les parefeux sont en haute disponibilité.

Ces choix technologiques sont précisément décrits dans l'offre du titulaire.

5.1.3 Exigences particulières pour le titulaire et le choix de son opérateur fibre dans le cas de l'offre de base

Le titulaire répond à l'offre de base décrite ci-dessous pour laquelle des exigences spécifiques sont exprimées :

Utilisation d'une infrastructure fibre optique existante

Afin de garantir une mise en œuvre rapide et d'éviter toute intervention complexe ou intrusive sur les infrastructures existantes :

- Le prestataire retenu devra obligatoirement utiliser l'une des lignes fibre optique actuellement disponibles dans le bâtiment sans installation d'une nouvelle ligne ou de nouveaux fourreaux.
- Les lignes disponibles sont signalées au niveau du sous-sol du bâtiment, où des arrivées opérateurs (Alphalink, ZAYO, COLT, SFR, Orange, BT, FREE) sont identifiées.

Préférence pour la fibre existante utilisée actuellement

- À titre de préférence, la ligne fibre opérée par **Alphalink** (co-traitant de l'hébergeur actuel) est entièrement fonctionnelle et prête à l'emploi.
- Le prestataire peut cependant opter pour une autre ligne disponible, sous réserve de s'assurer de sa compatibilité technique avec les services proposés.

Vérifications techniques préalables

- Le prestataire devra effectuer toutes les vérifications nécessaires pour garantir la faisabilité technique de l'utilisation de la fibre choisie (débit, disponibilité, connectivité, etc.).
- Une visite technique sur site, réalisée par un profil technique, sera organisée avant la remise des offres afin de permettre à chaque candidat de vérifier les installations.

Difficultés et accessibilité aux infrastructures

- La situation actuelle du chemin de câble est particulièrement délicate et restreint fortement d'installer de nouveaux fourreaux, câbles ou de tirer une nouvelle ligne fibre optique (chemin saturé, passage par la rue au travers des sous-sols d'un restaurant privé particulièrement difficile).

Justification dans l'offre

- Dans son mémoire technique, le prestataire devra indiquer clairement la ligne choisie, les étapes de vérification effectuées, ainsi que les modalités de collaboration avec l'opérateur concerné pour garantir le service attendu.

5.1.4 Exigences particulières pour le titulaire et le choix de son opérateur fibre : variante à la proposition précédente

Malgré la situation décrite, le titulaire peut répondre aux exigences par une offre différente.

Il est ici libre d'installer une nouvelle ligne fibre selon le chemin de câbles possible par les opérateurs.

Il respecte les délais de mise en œuvre ainsi que les exigences de débit et de stabilité exprimées plus haut dans le document.

Vérifications techniques préalables

- Le prestataire devra effectuer toutes les vérifications nécessaires pour garantir la faisabilité technique de l'utilisation de la fibre choisie (débit, disponibilité, connectivité, etc.).
- Une visite technique sur site, réalisée par un profil technique, sera organisée avant la remise des offres afin de permettre à chaque candidat de vérifier les installations.

Difficultés et accessibilité aux infrastructures

- La situation actuelle du chemin de câble est particulièrement délicate et restreint fortement d'installer de nouveaux fourreaux, câbles ou de tirer une nouvelle ligne fibre optique (chemin saturé, passage par la rue au travers des sous-sols d'un restaurant privé particulièrement difficile).

Justification dans l'offre

- Dans son mémoire technique, le prestataire devra indiquer clairement la ligne choisie, les étapes de vérification effectuées, ainsi que les modalités de collaboration avec l'opérateur concerné pour garantir le service attendu. Une attention particulière sera apportée aux modalités de mise en place de la ligne qui tient compte des difficultés fortes d'accès (chemin de câble, tier restaurateur, saturation des fourreaux et des emplacements de passage...).

5.1.5 Nomadisme et accès au système d'information de l'AFLD

Les collaborateurs de l'Agence spécifiés par l'AMOA SI de l'AFLD doivent avoir la capacité d'accéder au SI de l'AFLD en dehors des locaux de l'Agence grâce à un dispositif sécurisé VPN installé sur les postes clients et répondants aux exigences minimales suivantes :

- **Postes du domaine AFLD**
- **Authentification forte (double authentification) pour la connexion au VPN AFLD**

Le dispositif est supervisé et maintenu par le titulaire qui assure l'application des mises à jour critiques dans le mois qui suit la publication par l'éditeur/le fournisseur.

5.1.6 Dispositifs de sécurité de l'hébergeur

Le titulaire de l'hébergement met en œuvre un pare-feu dédié pour l'AFLD, **en haute disponibilité permettant notamment :**

- De contrôler les flux entrants et sortants WAN, LAN, InterLAN, vLAN
- De contrôler les flux web (web filtering)
- D'identifier et de contrôler les accès applicatifs (application control)
- De prévenir les virus et autres malwares
- De réaliser les reporting usuels

La technologie utilisée répond aux exigences de sécurité précisées dans le paragraphe 3 du document.

La haute disponibilité des pare-feux est exigée en entrée des DC de l'hébergeur ET en entrée de l'agence AFLD (2 x 2).

L'AFLD exige d'avoir à disposition les logs (journaux) générés par l'ensemble des équipements de sécurité (parefeu, vpn...) sur une période d'une année. Ces logs peuvent être stockées au sein d'un SYSLOG centralisé pour l'AFLD.

Le dispositif est supervisé et maintenu par le titulaire qui assure l'application des mises à jour critiques dans le mois qui suit la publication par l'éditeur/le fournisseur

Le titulaire permet un accès à l'interface d'administration du pare-feu au RSI de L'AFLD, en mode lecture.

La matrice des flux, le schéma réseau est fourni par le titulaire à la demande du RSI.

5.1.7 Licences Microsoft Windows, serveur & CAL

Le titulaire prend en charge la gestion et le cout (ou cout de location) des licences Windows server et CAL nécessaires pour le fonctionnement et les accès au SI AFLD.

5.2 Mise en place / Phase de cadrage / Plan de migration & Migration vers nouvelle infrastructure – prestation forfaitaire F01-HEB

Le marché d'hébergement en cours du SI AFLD et des liens de communication **arrive à échéance début août 2025**.

Le titulaire de ce marché effectue toutes les actions nécessaires afin de reprendre l'hébergement proprement dit du système informatique de l'Agence tel que décrit aux paragraphes 3.2.4, 3.2.5, dans les meilleures conditions de qualité de service et d'efficacité.

Le titulaire fournit également les liens de connectivité et les dispositifs qui assureront les accès de l'AFLD à son infrastructure et aux services attendus.

Cette période de mise en place est **d'une durée de 3 mois maximum** à compter de la date de notification de ce marché, selon les modalités définies au cahier des clauses administratives particulières.

L'AFLD met à la disposition du titulaire la documentation et les éléments en sa possession lui permettant d'appréhender le contexte.

5.2.1 Transfert des prestations

A partir de la situation existante, le titulaire détermine les conditions de transfert des prestations de l'hébergeur antérieur vers le titulaire, de telle sorte que les prestations basculent sous son entière responsabilité sans que son intervention puisse être à l'origine d'une interruption des services ou d'une dégradation de la qualité des services produits par l'hébergeur précédent.

L'hébergeur antérieur de l'AFLD était contractuellement engagé sur les points suivants :

- Transfert des documents
 - Dans le cadre d'un changement de prestataire, il s'est engagé à fournir à l'AFLD tous les documents et procédures nécessaires à la prise en main de la mission d'hébergeur.
 - Transfert de compétences
 - Il s'est engagé, pendant la période de transfert de compétence, à dialoguer avec le titulaire et à lui fournir tous les éléments nécessaires à la poursuite de la mission.
 - Transfert des connaissances
 - Afin d'encadrer le transfert des connaissances et sous la responsabilité de l'AFLD vers le titulaire, il est tenu de répondre à toute demande liée à la poursuite de la mission.
- ➔ Si l'AFLD valide une insatisfaction des transmissions des informations, elle pourra décider de prolonger la prestation de transfert de connaissances pour une durée égale à 1 mois.

5.2.2 Note de cadrage, PAQ, réunion de lancement et plan de migration

Le titulaire prend connaissance précisément de l'environnement AFLD, de l'infrastructure précise qu'il a à transférer au sein de son data center. Il élabore le plan de migration qu'il doit ensuite exécuter pour transférer dans les délais l'ensemble de l'infrastructure et ses services.

A cours de cette phase, le titulaire a en charge la rédaction de la note de cadrage, du plan d'assurance qualité (PAQ) et du plan de migration (étapes, impacts, risques). Il a également la charge de l'organisation **d'une réunion de lancement** avec les différentes parties du projet.

La note de cadrage a pour objectif d'affiner les exigences du présent cahier des charges en précisant les moyens et la méthode mis en œuvre par le titulaire pour y répondre. Ce document a valeur contractuelle. En annexe de ce document sont inclus le PAQ.

Une réunion de lancement est organisée par le titulaire dans un délai de sept (7) jours à compter de la notification du marché afin d'établir le chronogramme des actions à tenir pour prendre en charge l'hébergement. Ce document explique les phases opérationnelles et contient le tableau de bord de suivi opérationnel tout au long de cette mise en place. Il pourra évoluer en fonction des échanges et des décisions entre les parties.

Livrables :

- **Document opérationnel et tableau de bord de suivi issus de la réunion de lancement**
Délai : T0 + 10 jours
- **Note de cadrage et du PAQ**
Délai de livraison : T0 + 1 mois
La validation de la note de cadrage et du PAQ a lieu au plus tard à T0 + 3 mois = T1
- **PV installation et mise en route de l'ensemble des composants du SI AFLD au sein de la nouvelle infrastructure de l'hébergeur**
Délai : T0 + 3 mois (T1)

T0 est la date de notification du marché. Le cas échéant, les délais d'exécution mentionnés ci-dessus seront prolongés d'une durée égale à l'éventuelle prolongation de la phase de transfert de compétences.

L'élaboration de ces documents se fait dans le cadre d'un dialogue constant avec l'AFLD. La validation de la note de cadrage (et ses annexes) déclenche l'exécution des prestations de la phase opérationnelle de l'hébergement.

T1 est la date de validation de la note de cadrage (et du PAQ) et correspond à la date de démarrage de la phase opérationnelle d'infogérance.

5.3 Hébergement en mode opérationnel – prestation forfaitaire F02-HEB (T1)

5.3.1 Maitrise d'œuvre et pilotage de l'hébergement du SI

Les services attendus au titre du pilotage sont :

- L'élaboration, l'analyse et la communication à l'AFLD des éléments de pilotage. Le pilotage s'adosse à des tableaux de bords standards et élaborés mensuellement par le titulaire. Ils constituent le socle des échanges en comité et s'appuient sur des éléments factuels (outillage, log, etc.),
- Le pilotage des incidents en fonction de leur sévérité,
- Le contrôle qualité de la prestation (contrôle du respect du PAQ, du PAS, contrôle de la validité des référentiels documentaires et techniques, contrôle de la qualité des indicateurs, etc.),
- Le maintien à jour de la documentation qualité (PAQ, PAS), du plan et du référentiel documentaire de réversibilité,
- L'identification et le suivi des risques,
- Le conseil et le suivi d'amélioration continue,

5.3.1.1 Pilotage de l'hébergement, interlocuteurs exigés dans le cadre de la prestation

Le titulaire assure un rôle de direction et de coordination couvrant l'ensemble des prestations qui lui sont confiées.

Tout au long de la prestation, l'AFLD exige d'être en lien constant avec le titulaire et de bénéficier du dialogue régulier avec deux profils bien identifiés :

Le Titulaire désigne **un interlocuteur technique pour l'AFLD (ROC)** dont la mission principale est le pilotage et la coordination technique des prestations. Il :

- Possède une connaissance détaillée de l'environnement technique AFLD
- Veille au respect des règles de sécurité ;
- Assure la coordination technique de l'ensemble des prestations ;
- Propose des plans d'amélioration ou d'actions correctives ;
- Propose des améliorations techniques, des solutions et prend en compte les problématiques métiers de l'AFLD et ses exigences de sécurité
- A autorité pour prendre toutes les décisions opérationnelles courantes et urgentes.

C'est le référent technique de l'AFLD.

Il est présent lors des comités techniques réguliers.

Le titulaire désigne **un interlocuteur principal pour le contrat (SDM)** dont la mission principale est la coordination de l'ensemble des prestations fournies et le contrôle de la qualité de service. Il :

- Prend en charge le suivi administratif et financier du marché ;
- Est garant du respect des engagements et de la qualité de service ;
- Veille au respect des règles de sécurité ;
- Assure la coordination de l'ensemble des prestations ;
- Veille à la qualité opérationnelle du service ;
- Met en œuvre les moyens, garantit leur permanence, les adapte afin de respecter les engagements contractuels ;

Il est présent lors des comités techniques réguliers.

Le Titulaire désigne **un interlocuteur RSSI** dont la mission principale est d'intervenir sur tous les sujets liés à la sécurité du SI. Il :

- Est le RSSI référent au sein de l'entité du titulaire
Veille au respect des règles de sécurité ;
- Répond aux questions spécifiques sur la sécurité du SI que AFLD pourrait avoir au cours du marché (parfois en lien avec l'ANSSI) ;
- Propose des plans d'amélioration, des améliorations techniques ou des actions correctives dans ce domaine ;
- A autorité pour prendre toutes les décisions opérationnelles courantes et urgentes.

Il est présent selon le besoin lors des différents comités ou réunions spéciales traitant de la sécurité.

Le RSI et le responsable technique SI de l'AFLD sont les interlocuteurs principaux de l'Agence et ont autorité pour prendre les décisions courantes ou urgentes.

5.3.1.2 Devoir d'alerte, de conseil

Le titulaire est tenu à une obligation générale de conseil, d'information et de recommandation, et de mise en garde, sur le périmètre contractuel.

Le devoir de conseil et d'alerte auprès d'AFLD doit contribuer à l'amélioration de la performance du service et à la réduction des coûts des services associés. Le titulaire s'engage à émettre auprès de l'Agence tous les conseils et mises en garde nécessaires au cours de l'exécution du contrat notamment en termes de qualité de service, de continuité d'exploitation, **de sécurité et de mise à l'état de l'art et d'évolution**.

Il propose toute adaptation, amélioration, modernisation ou mise à niveau du SI qu'il juge souhaitable en vue d'optimiser les performances et les coûts de fonctionnement. Ceci s'applique aussi bien aux aspects techniques que méthodologiques ou organisationnels et s'appuie notamment sur l'analyse des indicateurs, la prise en compte des remontées clients et sur une gestion des problèmes (au sens ITIL du terme) permettant d'identifier les incidents récurrents afin de traiter les causes plutôt que les symptômes.

Dans le cadre de son obligation de conseil, le titulaire informe AFLD dès qu'il a connaissance de toute nouveauté technologique, ou nouveau produit ou service, plus adapté aux besoins d'AFLD en termes de coûts, de qualité des services ou de maîtrise des risques.

L'apport de conseil porte au minimum sur :

- Les technologies : tendances, opportunités, caractéristiques, valeur ajoutée, etc.,
- Les nouvelles versions et/ou les versions en place qui ne sont ou ne seront plus supportées,
- L'amélioration de l'organisation et de la coordination,
- Les opportunités de réduction de coûts,
- Les opportunités d'amélioration de la qualité des services,
- La sécurité du SI

La veille technologique est assurée par le titulaire. Il est attendu de ce dernier un apport important sur ces champs compte tenu de son expérience, de sa visibilité sur les contrats clients, et de ses capacités de mutualisation des moyens.

5.3.1.3 Plan d'Assurance Qualité

Le titulaire a la responsabilité de l'élaboration et de la mise à jour du PAQ qui recense l'ensemble des conditions d'exécution des prestations.

La liste suivante est une liste non exhaustive des points qui doivent être mentionnés dans le PAQ :

- Les interlocuteurs des parties
- Le fonctionnement du comité de pilotage technique
- Le fonctionnement ces cellules de crises
- Le reporting : tableaux de bord, indicateurs
- Les procédures d'incitation au maintien de la qualité
- Les normes de présentation des documents
- La documentation de l'architecture du système d'information
- La classification des applications par niveau de criticité
- Les processus et délais d'administration et d'exploitation
- Les processus et les délais d'alerte
- Les processus de gestion des incidents et des processus d'escalade
- Les processus de gestion des sauvegardes informatiques
- Les processus de demande de service exceptionnels
- Les processus et délais de demande, d'exécution, de recette des installations
- Les processus et délais de demande de changements,
- Les règles et processus de sécurité
- Les règles et les processus de réversibilité
- Les processus d'utilisation de l'outil de suivi du support

5.3.1.4 Plan d'assurance sécurité – PAS

Le titulaire élabore le plan d'assurance sécurité qui formalise précisément tous les dispositifs qu'il s'engage à mettre en œuvre pour répondre aux exigences de sécurité et de gestion des risques opérationnels sur le périmètre hébergé du système d'information de l'AFLD. 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.

5.3.1.5 Comités

Au titre des prestations du marché, le titulaire organise plusieurs réunions, notamment au début du marché. Parmi celles-ci figurent au moins :

- La réunion de lancement
- La réunion de fin de cadrage (T1)
- Un comité de suivi technique et opérationnel **hebdomadaire au début** du marché puis, après accord entre les parties, **mensuel**, qui traite les priorités, les échanges techniques, l'information utile, le planning à court et moyen terme. Les interlocuteurs sont à minima le SDM, le ROC. **La présence du référent technique est impérative** lors des COTECH.
- Un comité de suivi sécurité informatique, **trimestriel**, puis semestriel, qui traite les priorités, les échanges techniques, l'information utile, le planning à court et moyen terme

sur les aspects spécifiques liés à la sécurité du SI ; les interlocuteurs sont à minima le RSSI et le SDM.

- Des COPIL, à fréquence **semestriel** jusqu'à la fin du marché. Les interlocuteurs sont à minima le SDM et le responsable commercial du compte.

Le compte-rendu des différentes réunions est transmis par le titulaire dans un délai de 5 jours ouvrés à compter du lendemain de la réunion. L'AFLD dispose d'un délai de 5 jour ouvré à compter de la réception du compte-rendu pour approuver ou émettre d'éventuelles réserves auquel cas une nouvelle version sera émise par le titulaire, l'objectif étant de finaliser le compte rendu dans les 10 jours suivant la réunion.

5.3.1.6 Comité de pilotage

Le Comité de Pilotage est l'instance de pilotage contractuelle et décisionnelle. Il se réunit de façon mensuelle (sur le site de l'AFLD ou en visio ou audio conférence).

Sans que cette liste soit limitative, il :

- Contrôle la qualité des prestations effectuées par le titulaire, expose les indicateurs pertinents de suivi de la prestation
- Décide de plans d'améliorations,
- Suit l'avancement des projets,
- Préconise des évolutions de périmètre et des services,
- Décide de l'application et du quantum des pénalités appliquées,
- Prépare les orientations et les évolutions du Système d'Information de l'AFLD,
- Assure la gestion financière du contrat,
- Assure le suivi des documents contractuels révisables,

Le Comité de Pilotage est composé de représentants de chacune des Parties. L'ordre du jour et le document support à la réunion sont proposés par le titulaire à l'AFLD au plus tard 5 jours avant la réunion, l'AFLD pouvant faire des remarques au plus tard la veille de cette réunion. Le compte rendu est transmis par le titulaire dans un délai de 5 jours. L'AFLD dispose d'un délai de 5 jours à compter de la réception du compte-rendu pour approuver ou émettre d'éventuelles réserves auquel cas une nouvelle version sera émise par le titulaire, l'objectif étant de finaliser le compte rendu dans les 10 jours suivants la réunion.

L'ordre du jour des Comités de Pilotage intégrera notamment les éléments suivants :

- Les faits marquants de la période ;
- Une analyse commentée par le titulaire des tableaux de bord mensuels comprenant les indicateurs, les éléments de volumétrie, les éléments de sécurité ;
- Une revue des principaux changements et des mises en production du mois écoulé, ainsi que des prévisions à 3 mois ;
- Une revue d'avancement des projets ou études en cours (jalons, dates impératives, ...) ;
- Un suivi financier ;
- Une revue des risques ;
- Un suivi des préconisations issues des Rapports Incidents Techniques et de leur mise en œuvre en Comité Opérationnel ;
- Une fois par an, une vérification du Plan de réversibilité et du Plan d'Assurance Qualité (PAQ)

- Deux fois par an, une vérification du Plan d'Assurance Sécurité (PAS), du référentiel documentaire de réversibilité ;
- Validation des plannings.

5.3.1.7 Reporting

En début de chaque mois, le titulaire remet à l'AFLD un document de synthèse qui résume l'activité de la période, les progrès atteints, les dysfonctionnements constatés, leur analyse et les plans d'actions correctives.

Notamment, dans ce document, figurent plusieurs catégories d'information de reporting :

- Le volume d'activité
Les demandes traitées, les interventions sur site, les zones impactées (matériels, téléphonie, logiciels, métiers...).
- Le niveau de service
Informations relatives à l'appréciation de la qualité des prestations, mesures de la qualité des services
- L'utilisation des ressources techniques
Indicateurs de consommation de ressources techniques comme charge CPI, espace disque par application, espace disque données, BAL, bande passante réseau, visio...), évaluation des capacités disponibles permettant d'anticiper les extensions nécessaires.
- Les alertes/conseil/rappels
Information sur les actions à entreprendre, soit par le titulaire, soit par l'AFLD, pour le fonctionnement optimal du SI. Il peut s'agir par exemple du remplacement à planifier de telle ou telle machine serveur, du renouvellement des licences x, etc...
- Pannes, interruption de services
Informations sur les événements bloquant survenues lors de la période d'activité, de pannes importantes, nécessitant ou non une interruption de tel ou tel services et ou applications

Livrables :

- Cahier de synthèse de l'hébergement opérationnel
Délai : Avant le 10 de chaque mois

5.3.1.8 Validation des installations tierces

Le service informatique de l'AFLD est amené à installer de nouveaux produits (logiciels et/ou matériels) pour répondre aux besoins métiers (nouveaux projets tels que décrits dans ce document).

Le titulaire apporte son expertise et veille à ce que les prérequis techniques, les procédures d'installation et d'exploitation des outils ou solutions logicielles que l'AFLD envisage d'acquérir, sont conformes et compatibles avec le système informatique infogéré.

5.3.1.9 Documentation, mise à jour constante

Le titulaire doit fournir à l'AFLD, chaque année (date d'anniversaire de la prestation + 1 mois maximum), les versions mises à jour des documents suivants :

- Plan d'assurance qualité
- Plan d'assurance sécurité
- Plan de réversibilité

Et également :

- L'architecture du Système informatique de l'AFLD (schéma général, visio et description détaillée), DAT
- Le tableau des configurations des machines serveurs, types, OS, garanties, références des contrats de maintenance le cas échéant,
- La topologie réseau,
- Le tableau des comptes administrateurs incluant les mots de passe, qui gèrent les applications, les serveurs, les différents accès protégés, et que le titulaire aurait créé dans le cadre de sa mission

Livrables :

- **Excepté le PAQ, les documents sont livrés la première année au plus tard à T0+ 6 mois.**

5.3.2 Evolution du SI AFLD, Déploiement de nouvelle VM

Le titulaire prend en charge le déploiement d'une nouvelle VM à la demande du SI interne de l'AFLD. Cette capacité de déploiement doit proposer un nombre de templates de VM limité, à minima:

Pour Windows :

ID	RAM (Go)	vCPU (Nb)	DISK (Go)	Disk Type
Low normal	6	2	80	HDD
Medium normal	12	4	200	HDD
High normal	16	8	1000	HDD
Low SSD	6	2	80	SSD
Medium SSD	12	4	200	SSD
High SSD	16	8	500	SSD

Les couts relatifs à la prise en charge de ces VMs supplémentaires sont stipulés dans le cadre de réponse financier. Ces prix comprennent la mise en œuvre, la puissance spécifiée, la ou les licences Windows le cas échéant, l'antivirus serveur et les autres dispositifs logiciels propres à l'hébergeur pour permettre son fonctionnement, son accès, sa maintenance.

Pour chacun de ces templates, le cout supplémentaire de ressources ajoutées (disque, RAM ou cpu) est également indiqué dans le bordereau de prix unitaires, par exemple :

Ajout de ressource	
vCPU (Nombre)	1
RAM (Go)	2
Disque HDD (Go)	100, 500 et 1 To
Disque SSD (Go)	100, 300 et 500

Pour Linux :

La démarche attendue est identique à celle exposée pour Windows.

5.3.3 L'administration et l'exploitation des systèmes

L'exploitation des systèmes est l'ensemble des activités récurrentes assurant le fonctionnement des systèmes informatiques en environnement de production ; l'administration des systèmes est l'ensemble des activités récurrentes contribuant à maintenir opérationnel l'environnement d'exploitation.

5.3.3.1 Généralités

Le titulaire mesure et maintient la qualité de service attendue. Les attentes de l'AFLD en matière de qualité de service sont précisées au chapitre traitant de la convention des services.

Les activités récurrentes couvrent au minimum les fonctions suivantes :

- Gestion des configurations des systèmes
- Gestion des menaces virales (mise en place de solution antivirus sur l'ensemble des serveurs hébergés, prévention des malwares et cryptolocker)
- Pilotage des serveurs
- Gestion des incidents d'exploitation sur les serveurs (panne totale d'un serveur, écran bleu...)
- Gestion des sauvegardes/restaurations (cf politique de sauvegarde décrite dans le document)
- Applications des procédures prévues en matière de sécurité (PAS)
- Gestion des performances des systèmes (surveillance des alertes...)

5.3.3.2 Description des prestations

Administrations des systèmes

- Gestion des sauvegardes :
 - Réaliser et contrôler la bonne exécution de la sauvegarde des données selon la politique définie,
 - Garantir la récupération des données de l'AFLD en cas de perte ou d'altération,
 - Préconiser les évolutions souhaitables (support de stockage, outils de sauvegarde ou de restauration...) et les mettre en œuvre si elles sont validées avec l'AFLD,
 - Réaliser les tests de sauvegarde.
 - Réaliser les tests de restauration

Exigences minimales de la politique de sauvegarde de l'AFLD :

Les sauvegardes opérées suivent la politique suivante :

- 6 sauvegardes Quotidiennes et immuables par semaine avec une rétention de 7 jours
 - 1 sauvegarde Hebdomadaire par semaine avec une rétention de 27 jours
 - 1 Copie Mensuelle de la première sauvegarde Hebdomadaire, avec une rétention de 52 semaines.
 - La première sauvegarde hebdomadaire de l'année civile est copiée sur bandes LTO et envoyée à l'Agence Française de Lutte contre le Dopage.
-
- Mise à niveau des logiciels de base :
 - Surveiller en continu H24 7/7 les performances des systèmes,
 - Traiter les alarmes et les événements en provenance de la machine,
 - Analyser périodiquement les statistiques relatives aux performances,
 - Préconiser les évolutions souhaitables de configuration ou d'architecture
 - Gestion des sécurités :
 - Concevoir, mettre en place et maintenir à jour les dispositifs et les procédures de prévention, de détection et d'élimination des atteintes à la sécurité des systèmes informatiques (accès non autorisés, attaque virale, attaque malware , ...) pour l'intégralité du système d'exploitation ;
 - Conseiller le SI AFLD sur la gestion de la sécurité des applications, accès et modifications des sources, gestion des habilitations,
 - **Assistance** dans le cadre de la réception et la mise en production des nouvelles applications ou versions d'applications (applications métiers, spécifiques éditeurs, hors OS)
 - L'organisation des installations des nouvelles applications ou version logicielles est prise en charge par l'équipe SI interne de l'AFLD. Le titulaire assiste l'AFLD sur le volet technique et notamment dans les aspects suivants :
 - Aider au contrôle des performances systèmes des applications :
 - Surveillance des services windows et base de données
 - Non dégradation des performances des autres éléments des systèmes (autres applications, réseau...)
 - Disponibilité des ressources nécessaires (espace disques, RAM, autres support...)

Exploitation des systèmes

- Pilotage des serveurs :
 - Superviser le bon fonctionnement des serveurs (taux d'occupation mémoire, CPU...),
 - Superviser les disques : vérification de l'intégrité des disques, suivi du taux d'occupation,
 - Prendre toute mesure préventive de nature à éviter tout blocage d'un serveur,
 - Préparer le tableau de bord mensuel du fonctionnement des serveurs permettant la mesure d'indicateurs de niveaux de service.

- Application des procédures de sauvegarde :

En fonction des procédures définies en administration des systèmes :

- Identifier les supports de sauvegarde,
- Réaliser les sauvegardes conformément à la stratégie de sauvegarde (voir le rappel plus haut),
- Résoudre les incidents survenant en cours de sauvegarde,
- Restaurer les fichiers systèmes et/ou utilisateurs en cas de nécessité,
- Archiver et stocker les supports,
- Procéder régulièrement (au moins 2x l'an) aux tests de restauration de données.

- Application des procédures prévues en matière de sécurité :

- Enregistrer et traiter les alarmes provenant des dispositifs informatiques de sécurité (ex. : parefeu), des dispositifs anti intrusions et antivirus ; appliquer les procédures prévues,

Pour rappel, les journaux (fichiers logs, archives) des systèmes de sécurité doivent être stockés et accessibles sur une durée légale d'une année. L'AFLD peut demander à tout moment la mise à disposition de ces journaux.

5.3.4 L'administration et l'exploitation des réseaux

5.3.4.1 Généralités

Tous les équipements réseaux, fournis par le titulaire (réseau LAN, réseau WAN, VPN, accès internet) et recensés dans le schéma d'architecture global font partie du périmètre d'administration et d'exploitation du titulaire.

Au minimum, les activités récurrentes à la charge du titulaire sont :

- Administration de tous les éléments actifs
- Exploitation et supervision des éléments actifs
- Gestion des sécurités
- Evolutions (firmware,....)
- Gestion et administration des liens d'interconnexion
- Gestion et administration de l'accès internet

5.3.4.2 Description des prestations

- Administration des éléments actifs :
 - Paramétrage (reprise du paramétrage initial et évolutions),
 - Sauvegarde des environnements,
 - Prise en charge du matériel de secours (spare) éventuel,
 - Mise à jour des matériels et logiciels,
 - Etude et mise en œuvre des évolutions.

- Exploitation, supervision :
 - Superviser les éléments actifs du réseau (routeurs, commutateurs...), récupérer et traiter les alertes, collecter les statistiques de fonctionnement,
 - Résoudre les incidents : traiter les alertes, mettre en œuvre les procédures d'escalade, résoudre l'incident ou déclencher l'intervention d'un tiers (opérateur, mainteneur...),
 - Préparer le tableau de bord mensuel du fonctionnement des réseaux (mesures de disponibilité, mise en évidence des occurrences de saturation),
 - Contrôler le fonctionnement des liaisons de toutes natures (liaisons Ethernet tout débit) hors périmètre des opérateurs de télécommunications, notamment en cas d'incident et en recette de modifications réseau,
 - Respecter les mesures préventives existantes afin d'éviter les blocages d'éléments actifs.
- Gestion des sécurités :
 - Concevoir, mettre en place et maintenir les dispositifs et procédures de prévention, détection et élimination des atteintes de sécurité des réseaux (accès non autorisés, attaques virales, autres tentatives...),
 - Contrôler et suivre les infractions de sécurité.

5.3.5 La gestion des changements informatiques

On appelle changement toute opération non récurrente qui s'avère nécessaire pour maintenir le SI opérationnel en respectant les engagements sur les niveaux de services précisés au chapitre correspondant.

Tout changement nécessite un délai de préavis.

Ce délai est la durée entre la transmission au titulaire d'une demande de changement à venir, et la prise d'effet dudit changement avec son intégration dans le périmètre d'exercice des prestations du titulaire.

Les procédures de recette sont décrites dans le PAQ.

5.3.6 La supervision des systèmes et des réseaux

Le titulaire prend en charge la supervision du SI mise à disposition de l'AFLD. **Il est attendu du titulaire qu'il privilégie les actions proactives plutôt que de réagir uniquement sur les incidents constatés.**

5.3.7 Prestations annexes

Les prestations annexes correspondent à des prestations non comprises dans les prestations de base de l'hébergement (prestations à prix global et forfaitaire). Elles sont déclenchées, si le besoin apparaît, par bon de commande.

Les prestations annexes font l'objet de commandes d'unités d'œuvre décrites et chiffrées dans le bordereau des prix unitaires.

Elles permettent de répondre à tout projet d'envergure initié par l'AFLD, sur les conseils ou non du titulaire, nécessitant une phase d'étude détaillée et ayant une incidence sur le système d'information de l'AFLD.

Tout projet de ce type donne lieu à une étude préalable réalisée par le titulaire pour évaluer une enveloppe en termes de charge de travail, de délai et de budget.

Le titulaire propose une typologie des intervenants susceptibles d'intervenir pour la mise en œuvre de ces prestations (formateur, chef de projet, technicien, ingénieur).

Au titre de l'obligation de conseil mise à la charge du titulaire, cette étude préalable est comprise dans les prestations de base de l'hébergement.

Ces prestations annexes sont à traiter comme des projets à part entière.

- Les prestations annexes portent sur :
 - Transfert important d'équipements d'un site à un autre (déménagement),
 - Prestation d'assistance et de conseil hors périmètre,
 - Projet de migration majeure (nouveau service critique à héberger)
 - Travaux d'études et de réalisations spécifiques dans le cadre d'une évolution majeure du SI de l'AFLD.
- Ne relèvent pas des prestations annexes mais sont comprises dans le périmètre de base de l'hébergement (liste non exhaustive) :
 - La réinstallation d'un serveur physique ou virtuel existant,
 - Installation d'un nouveau serveur physique,
 - L'installation d'un nouveau serveur virtuel,
 - La réinstallation d'un serveur virtuel existant,
 - Les conseils courants,

6 Convention de services, disponibilité et réversibilité applicable à tous les lots

Les niveaux de services recensés dans ce chapitre sont l'expression des besoins de l'AFLD.

Les définitions suivantes sont reprises dans le PAQ et servent à définir les indicateurs de la prestation.

6.1 Disponibilité du système informatique

La disponibilité d'un système informatique est l'état au cours duquel un utilisateur de ce système peut accéder aux fonctions qui lui sont autorisées et en faire un usage normal pour en retirer les résultats conformes à ceux que le système est prévu de produire.

Pour un utilisateur donné, le système informatique est donc considéré comme disponible si l'utilisateur dispose de l'ensemble des fonctionnalités (système central opérationnel, données à jour, poste de travail en service) lui permettant d'en faire un usage complet.

6.2 Résolution d'incident

Il s'agit du rétablissement total de l'état initial du système informatique, avant son incident.

6.3 Limite de responsabilité

Les niveaux de service et les performances du titulaire sont appréciés sur les seules prestations qui lui incombent. Les délais et taux de satisfaction des délais demandés pour la résolution d'un incident ne concernent que les incidents dont la résolution met en œuvre uniquement des prestations confiées au titulaire. Pour les autres incidents, les délais et taux de satisfaction des délais sont appréciés sur les seules prestations du titulaire, si possible.

6.4 Niveau de service constaté et niveau de service garanti

On distingue pour certains indicateurs, le niveau de service constaté du niveau de service garanti.

Ainsi, le niveau de service constaté est mesuré quelles que soient les limites de responsabilité du titulaire. C'est le reflet de la réalité telle que vécue par les utilisateurs AFLD.

Le niveau de service garanti est obtenu par élimination du niveau de service constaté, des effets sur la mesure de l'indicateur, d'actions dont le déroulement n'est pas placé sous la responsabilité du titulaire. Par exemple il s'agirait du délai de rétablissement d'une télécommunication si le réseau était hors périmètre de l'infogérance.

L'engagement du titulaire sur les niveaux de service constatés est un engagement de moyens : tout mettre en œuvre pour suivre et relancer les tiers n'ayant pas eux-mêmes d'engagement de résultats envers le titulaire.

L'engagement du titulaire sur les niveaux de service garantis est un engagement de résultats dont le respect est vérifié par rapport aux indicateurs, valeurs cibles contractuelles.

6.5 Heures de service normales

Les heures de service normales de l'AFLD sont de **07H30 à 18H30**, du lundi au vendredi.

6.6 Heures de service étendues

Les heures de service étendues de l'AFLD sont de **05H00 à 07H30** et de **18H30 à minuit**, du lundi au vendredi, et de 05H00 à minuit le samedi et dimanche pour les services critiques.

6.7 Criticités des applications

La criticité traduit l'importance de d'une application dans le métier de l'AFLD.

On considère 3 niveaux :

- Criticité 1

Le dysfonctionnement d'une application avec ce niveau de criticité peut avoir un impact fort sur le niveau de service et le fonctionnement de l'agence. Le nombre d'utilisateurs ou de services affectés est généralement important.

- Criticité 2

Le dysfonctionnement d'une application avec ce niveau de criticité a un impact moyen ou faible sur le fonctionnement de l'agence. Le nombre d'utilisateurs ou de services affectés est généralement peu important.

- Applications sans criticité associée

Autres applications. Le titulaire s'efforce d'en assurer la disponibilité sans que des pénalités ne soient applicables.

La qualification actuelle des applications par niveau de criticité peut évoluer dans le temps en fonction notamment de l'acquisition de nouvelles applications ou de l'évolution du périmètre fonctionnel d'applications existantes, sans impact sur le montant des prestations forfaitaires du titulaire.

La classification des applications par niveau de criticité est établie et tenue à jour dans le PAQ.

☞ L'évolution de criticité d'une application est décidée par l'AFLD et le titulaire définit alors les impacts sur l'organisation du système informatique lui permettant de respecter ses engagements de niveau de service correspondant.

On donne ici la liste des applications existantes et leur criticité associée :

Application	vLAN	Métier	Niveau de criticité
GFI PEP / GBCP	PROD	Comptable	2
Messagerie Exchange AFLD	PROD	Collaboratif	1
Réseaux, LAN, WAN, WLAN, FW	PROD	Communication	1
Serveurs de fichiers	PROD	Accès aux données "entreprise"	1
Active Directory, NPS,	PROD	Annuaire, sécurité	1
MAGELLAN – MAGELLAN GC	PROD	Métier dédié contrôle	1

6.8 Indicateurs de la disponibilité

6.8.1 Mesure de la disponibilité

La disponibilité d'une application (plus largement l'ensemble des composants concourant à son bon fonctionnement) est mesurée sur la plage des heures de service normales et étendues, hors arrêt planifiés.

La disponibilité d'un système résulte des disponibilités simultanées :

- Du serveur de production sur lequel est exploitée l'application,
- De la base de données associée le cas échéant,
- Des systèmes éventuels de communication associés.

La disponibilité attendue des systèmes applications dépend de la criticité des applications.

Si un système comprend plusieurs applications de niveaux de criticité différents, la disponibilité attendue de ce système est celle qui correspond au niveau de criticité le plus élevé.

Le titulaire tient à jour, pour chaque application, la liste des composants (serveurs, base de données, système de communication...) dont la disponibilité concurrente conditionne la disponibilité de l'application.

Les serveurs n'hébergeant que des applications classées « hors production » sont eux-mêmes classés « hors production ». Ils ne sont donc pas soumis aux garanties de services et aux pénalités. Le titulaire s'efforce cependant d'en garder la disponibilité.

6.8.2 Définition des arrêts planifiés

L'AFLD définit les périodes d'arrêts planifiés de la manière suivante :

- Les arrêts pour intervention technique à la demande du titulaire sont planifiés 5 jours ouvrés à l'avance avec l'accord de l'AFLD.
- Ces arrêts ne peuvent dépasser 12 heures par mois et par système et sont choisis pendant les périodes d'inactivité ou de très faible activité du système concerné.
- Un arrêt planifié ne peut excéder 4 heures continues (de service normal) pour les applications de criticité 1, 8 heures continues pour les applications de criticité 2.
- Les arrêts pour intervention demandée par l'AFLD sont planifiés par celle-ci

6.9 Engagement de disponibilité de l'infrastructure et des applications, exigence sur les sauvegardes, exigence d'évolutivité et de liaison entre les sites.

6.9.1 Politique de sauvegarde des données AFLD

Le serveur de gestion des sauvegardes est hors du domaine AFLD et **suit les principes des règles de sécurité de l'ANSSI** concernant les sauvegardes des données :

- Serveur de sauvegarde cloisonné, et hors réseau de production de l'AFLD
- Serveur hors domaine windows (AD) de production
- Les flux de sauvegarde transitent au sein du réseau spécifique d'administration de l'hébergeur
- Règle 3-2-1 : 3 copies des données : 1 données de production + 2 copies sur 2 supports différents dont 1 hors ligne
- Les comptes admin pour la sauvegarde sont nominatifs et dédiés.

Les sauvegardes opérées suivent la politique suivante :

- 6 sauvegardes Quotidiennes et immuables par semaine avec une rétention de 7 jours
- 1 sauvegarde Hebdomadaire par semaine avec une rétention de 27 jours
- 1 Copie Mensuelle de la première sauvegarde Hebdomadaire, avec une rétention de 52 semaines.
- La première sauvegarde hebdomadaire de l'année civile est copiée sur bandes LTO et envoyée à l'Agence Française de Lutte contre le Dopage.

6.9.2 Exigences de disponibilité, d'évolutivité et d'un site de secours

L'AFLD exige les conditions suivantes concernant l'infrastructure mise en place par le titulaire hébergeur :

L'ensemble de la puissance informatique fournie pour satisfaire le périmètre défini dans le LOT hébergement reposera sur une infrastructure en haute disponibilité :

- Le titulaire assurera un dispositif de stockage redondant et distribué, assurant flexibilité et évolutivité.
- L'architecture est basée sur la mise à disposition de plusieurs nœuds (ESX, Hyp...). La perte d'un nœud complet est possible sans altérée aucunement la disponibilité des systèmes.
- Le DC (Data Centre) de production qui hébergera le SI AFLD assure un **RPO=0 en cas de perte d'un équipement** (nœud serveur, stockage, FW...)
- Le temps de rétablissement du service ne peut dépasser 10 minutes ; **RTO = 10 minutes**

Sur la durée contractuelle maximale du marché, le titulaire assure **une infrastructure pouvant absorber une augmentation de capacité de 15%**. (Stockage, CPU, RAM).

Le titulaire s'assure de sauvegardes immuables du SI de l'AFLD protégeant de toute attaque de cryptolocker. Les sauvegardes sont géographiquement lointaines du DC de production (>150 kms).

Le titulaire garantit un accès réseau permettant la redondance efficiente des données (Site principal, site de secours, site des sauvegardes).

L'AFLD demande la mise en place d'un site de secours activable par décision commune et en réponse à un incident majeure rendant indisponible le site principal de production.

Les systèmes installés sur le PRA sont ceux définis par la criticité 1.

L'infrastructure mise en place pour supporter ce PRA doit répondre à un **RPO = 1H** et un **RTO de 4H**.

Cas spécifique d'une attaque par cryptolocker.

Dans le cas spécifique d'une attaque par cryptolocker et propagée au niveau du PRA, le titulaire agit en mettant tous les moyens pour rétablir le DC principal et le PRA.

La dernière sauvegarde immuable () est alors considérée. Les systèmes de criticité 1 de l'AFLD sont prioritairement remis en fonction.

Le délai attendu de remise en fonctionnement des accès des éléments critiques est **24 heures**.

6.9.3 Plan PRA, Vérification, tests, suivi du plan

Le titulaire établit le plan de déclenchement du site de secours. Il s'assure qu'il est tenu à jour tous les ans et s'assure de réaliser des tests de fonctionnement.

Le titulaire fournit régulièrement un rapport prouvant que les sauvegardes immuables sont exploitables. Des tests de restauration sont régulièrement exécutés.

Le document contient à minima les chapitres suivants

- Objectifs et périmètre
- Politique de gestion des sinistres, critères
- Équipe de gestion de crise
- Inventaire des ressources et des services
- Scénarios de sinistres envisagés
- Procédures de déclenchement
- Procédure technique de basculement
- Communication et gestion des parties prenantes
- Tests et validation
- Documentation et mise à jour

6.10 Phase de réversibilité

6.10.1 Garantie de réversibilité

Le titulaire doit fournir à l'AFLD un plan de réversibilité lui permettant de reprendre sans difficultés, ou de faire reprendre par un tiers désigné par elle, les prestations fournies par le titulaire et ce, dans les meilleures conditions.

La durée de la phase de réversibilité est fixée à 3 mois minimum avant le terme du marché, quelle qu'en soit le motif.

6.10.2 Création et mise à jour

Le plan décrivant les modalités opérationnelles du processus de réversibilité est réalisé par le titulaire avant T1 + 3,5 Mois. Le document est mis à jour tous les ans par ce dernier. Après chaque mise à jour, il est soumis à validation de l'AFLD.

6.10.3 Contenu

Le plan de réversibilité décrit au minimum les points suivants :

- Le périmètre d'application du plan
- Les conditions générales d'exécution des opérations de réversibilité, notamment :
 - L'organisation à mettre en place et les responsabilités des parties
 - Les phases de mise en œuvre de la réversibilité
 - Les contraintes de planning et les jalons clefs, notamment la date de fin prévue de la prestation (ou date de basculement)
 - Les engagements en matière d'assistance technique et de formation
 - Les différentes options de réversibilité

- Le contrôle de la mise en œuvre de la réversibilité
- Les principes de la mise à jour et du contrôle du plan de réversibilité
- Les données et les informations à transmettre
- Les moyens matériels et logiciels à transférer

6.10.4 Obligations de fin de l'accord-cadre

Au terme de l'accord-cadre (terme, résiliation ou autre cas), le titulaire communique à l'AFLD les informations qui lui sont nécessaires pour lui permettre de préparer la réversibilité.

Ce droit s'exerce pendant la durée de 6 mois précédent le terme du marché ou à partir de la notification de la décision de résiliation.

A la date effective de fin de l'accord-cadre, le titulaire tient à la disposition de l'AFLD :

- Les moyens matériels et logiciels mis à disposition du titulaire pour autant que ces moyens subsistent à l'expiration du contrat,
- Les applications spécifiques de l'AFLD,
- La documentation opérationnelle dans sa dernière version et l'ensemble des documentations tenues à jour par le titulaire, ainsi que tout document ou élément qui aurait été mis à disposition du titulaire par l'AFLD.

Le titulaire apporte à l'AFLD (ou à tout tiers désigné) son assistance technique, notamment par le transfert des informations nécessaires, pour faciliter la reprise des prestations confiées.

☞ **Livrables à remettre : Plan de réversibilité**

Mises à jour du plan de réversibilité

Délai : T1 + 3,5 mois (plan), puis mise à jour tous les ans.

6.10.5 Mise en œuvre

La mise en œuvre du plan de réversibilité fait l'objet d'une commande d'unité d'œuvre décrite et chiffrée dans le cadre de réponse financier.

Le titulaire n'est dégagé de ses obligations au titre du contrat qu'après la signature par les deux parties d'un PV de recette de la réversibilité. Ce PV peut concerner l'ensemble des prestations de réversibilité, ou être décomposé en plusieurs PV correspondant aux étapes successives de la réversibilité, étapes qui auront été prévues et décrites dans le plan de réversibilité.

☞ **Livrables à remettre : PV de recette de réversibilité**

Délai : 1 mois avant le terme de l'accord-cadre

6.10.6 Information et conseil

Le titulaire a une obligation de conseil de l'AFLD dans le cadre de l'exécution du présent accord-cadre. Il s'engage à informer le représentant de l'AFLD de tout événement ou de toute difficulté de nature à compromettre la qualité de la prestation objet du présent marché.

6.10.7 Obligations de l'AFLD

Pour la bonne exécution des prestations, l'AFLD s'engage à collaborer activement avec le titulaire en lui communiquant dans les délais compatibles avec les délais d'exécution toutes les informations, les documents, les renseignements et les éléments existants qui sont utiles à l'exécution de sa prestation.