

Cahier des Clauses techniques Particulières Marché à procédure adaptée

Le pouvoir adjudicateur :

OFDT

69, rue de Varenne 75007 Paris

Objet du marché :

Infogérance du système d'information

Auteur (AMO)	Thomas HEBERT DIMOXILO
Date de mise à jour	13/01/2025 14:21
Version	CCTP_INFOGERANCE_v2.0.docx

Table des matières

1.	CONTEXTE.....	5
1.1.	Présentation	5
1.2.	Objet.....	5
1.3.	Contexte	5
2.	EXISTANT	6
2.1.	Personnel.....	6
2.2.	Volumétrie.....	6
2.3.	Serveurs.....	6
2.4.	Sauvegarde	6
2.5.	Téléphonie IP.....	6
2.6.	Firewall	7
2.7.	Réseau	7
2.8.	Wifi	7
2.9.	Messagerie	7
2.10.	Antivirus.....	7
2.11.	Bureautique.....	7
2.12.	Progiciels (VM).....	7
2.13.	Helpdesk / Gestion parc	9
2.14.	Documentation.....	10
2.15.	Projets à venir.....	10
3.	PERIMETRE D'INTERVENTION	11
3.1.	Référent technique.....	11
3.1.1.	Périmètre.....	11
3.1.2.	Attentes	11
3.1.3.	Tâche type	11
3.2.	Postes clients – Assistance utilisateurs	11
3.2.1.	Périmètre.....	11
3.2.2.	Attentes	11
3.2.3.	Tâches types	11
3.3.	Administration système	11
3.3.1.	Périmètre.....	11
3.3.2.	Attentes	12

3.3.3.	Tâches types	12
3.4.	Administration réseau	12
3.4.1.	Périmètre.....	12
3.4.2.	Attentes	12
3.4.3.	Tâches types	12
3.5.	Mises à jour	13
3.5.1.	Périmètre.....	13
3.5.2.	Attentes	13
3.5.3.	Tâches types	13
3.6.	Sauvegarde	13
3.6.1.	Périmètre.....	13
3.6.2.	Attentes	13
3.6.3.	Tâches types	13
3.7.	Anti-Virus et sécurité.....	14
3.7.1.	Périmètre.....	14
3.7.2.	Attentes	14
3.7.3.	Tâches types	14
3.8.	Applicatifs	14
3.8.1.	Périmètre.....	14
3.8.2.	Attentes	14
3.8.3.	Tâches types	14
3.9.	Messagerie	14
3.9.1.	Périmètre.....	14
3.9.2.	Attentes	14
3.9.3.	Tâches types	15
3.10.	Supervision	15
3.10.1.	Périmètre.....	15
3.10.2.	Attentes	15
3.10.3.	Tâches types	15
3.11.	Documentation.....	15
3.11.1.	Périmètre.....	15
3.11.2.	Attentes	16
3.11.3.	Tâches types	16
4.	GOUVERNANCE	17

4.1.	Suivi des interventions - ITSM	17
4.2.	Inventaire - ITSM	17
4.3.	Interlocuteur privilégié.....	17
4.4.	Rapport d'activité	17
4.5.	Comité de pilotage	18
5.	ENGAGEMENTS CONTRACTUELS.....	19
5.1.	Plage de service garanti (PSG)	19
5.2.	Garantie de Temps de Rétablissement	19
5.3.	Définition des niveaux de criticité.....	19
5.4.	Accès.....	19
5.5.	Fin de contrat	19
6.	MODALITE D'INTERVENTION.....	20
6.1.	Déplacements.....	20
6.2.	Intervention sur site / distante.....	20
7.	PARTIE FORFAITAIRE (DPGF)	21
7.1.	Coût infogérance	21
8.	BORDEREAU DES PRIX UNITAIRES	22
8.1.	Prix unitaires additionnels.....	22
8.2.	Initialisation de la mission	22
8.3.	Sauvegarde externalisée	22
8.4.	Licences	23
8.4.1.	Licence antivirus poste client	23
8.4.2.	Constitution dossier de site.....	23
8.4.3.	Licence antivirus serveur.....	23
8.5.	Profils.....	23
8.5.1.	Technicien.....	23
8.5.2.	Administrateur système junior.....	23
8.5.3.	Administrateur système senior	24
8.5.4.	Administrateur réseau.....	25
8.5.5.	Chef de projet.....	25
8.5.6.	Câblage	25

1. CONTEXTE

1.1. Présentation

L'Observatoire français des drogues et des tendances addictives (OFDT) est l'organisme public qui en France est chargé du recueil, de l'analyse et de la synthèse des données relatives aux drogues, qu'elles soient licites (alcool, tabac) ou illicites, ainsi qu'aux données sur les jeux d'argent et de hasard.

Créé en 1993, l'OFDT est un groupement d'intérêt public (GIP) à durée indéterminée, constitué entre dix ministères, la Fédération nationale des observatoires régionaux de santé (FNORS) et la Mission interministérielle de lutte contre les drogues et les conduites addictives (MILDECA), représentant l'État.

Le GIP est reconnu comme opérateur public dont la tutelle administrative est assurée par la MILDECA.

1.2. Objet

La présente consultation a pour objectif de permettre à la collectivité de

- Assurer l'infogérance du système d'information
- Bénéficier d'expertise technique informatique ponctuelle en fonction de ses besoins.

1.3. Contexte

Le marché actuel se termine en juin 2025 et doit donc être remis en concurrence.

Le maître d'ouvrage souhaite le renouveler dans des conditions similaires afin de pouvoir continuer de s'appuyer sur un partenaire en charge de l'ensemble de son système d'information.

2. EXISTANT

2.1. Personnel

En interne un agent non informaticien assure le rôle de référent pour la partie système d'information. Il ne peut toutefois être considéré comme une ressource technique interne et ne réalise aucune intervention technique.

2.2. Volumétrie

Ces données sont données à titre indicatif pour l'évaluation du coût d'infogérance. Elles n'ont pas de caractère contractuel.

Nombre d'agents	35
Nombre de compte Active directory	50
Nombre de compte Office 365	40
Nombre de poste client	70
Dont OS Windows	100%
Dont MacOS	0
Dont PC fixe	40
Dont PC portables	30
Téléphones mobiles	6
Téléphones IP SIP	30
SDA	60
Copieurs (location avec maintenance)	1

Les postes sont alloués aux agents dont une majorité dispose en plus de leur poste sur site d'un poste à domicile dans le cadre du télétravail.

2.3. Serveurs

- 2 Serveurs DELL / baie de disque DELL EMC
- Hyper V sans cluster (sur les 2 serveurs physiques, sans cluster)
- Serveurs 100% virtualisés
- Serveurs virtuels (Windows Server 2019 std)
 - DC, GFI (Applicatifs), PMB (Applicatif), Serveurs de fichier
 - OS Linux : Webcrawling et SINTES (Applicatif)

2.4. Sauvegarde

- Sauvegarde locale vers 1 NAS (QNAP)
- Sauvegarde externalisée illimitée (des VM).
- En marque blanche portée par le titulaire actuel (Appliwave / EuroFiber)
- Vade Secure MS 365 User (x35)

2.5. Téléphonie IP

- IPBX virtualisé Mylstra – Softphone Integral Voice - V 1.4.5.
- En marque blanche portée par le titulaire actuel
- 60 SDA
- Gérée et maintenue par un prestataire dédié (EuroFiber)

A court terme l'ensemble de la téléphonie IP sera supprimé, remplacée par un parc de téléphone mobile. (hors périmètre de l'infogérant)

2.6. Firewall

- Sophos XGS 136 Xstream

2.7. Réseau

- 3 Switchs Aruba

2.8. Wifi

Actuellement environ 3 bornes sophos sont déployées.

2.9. Messagerie

- Office 365 Exchange Online Plan 2 (x35)
- Microsoft 365 Business Basic (x5)

2.10. Antivirus

- Bit defender

2.11. Bureautique

Microsoft Office 2012 OEM

2.12. Progiciels (VM)

Réparti sur 2 Hyper-V distincts. (2 serveurs physiques)

WIN M9 / INETUM : pour la comptabilité, les immobilisations

GRH.net / INETUM : pour la paie

PMB : 1 instance SIGB PMB version 7.5.1 avec portail Pagéo (<https://bdoc.ofdt.fr>), VM Microsoft Windows Server 2019 Standard (4 CPU/12 Go RAM/ 400 Go d'espace disque). Mises à jour effectuée à distance par l'éditeur du SIGB, certificat SSL Let's Encrypt.

VM opnsense en Python, OS FreeBSD gérant les accès aux applications (fait office de proxy-serveur et de pare-feu)

VM OS Linux Debian 12 gérant les accès SSH aux différentes applications web

VM OS Linux Debian 12 hébergeant 2 applications web développement interne (<https://base-produits.sintes-lab.fr> et <https://sintes-lab.fr>) comprenant chacune une base de préproduction et une base de production PostgreSQL

VM CRAWLER, Développement interne (<https://crawler.sintes-lab.fr>) en Python, comprenant une base PostgreSQL dont la fonction est de crawler le web pour alimenter l'application <https://base-produits.sintes-lab.fr>

Quelques précisions

Les bases PostgreSQL sont conteneurisées avec Docker

Les applications sont gérées sur une seule VM Debian 12, sur laquelle fonctionne Docker. Chaque instance (sintes, base-produit, crawler, et leurs instances pré-prod respectives) fonctionne dans un conteneur Docker distinct, et sont gérés par docker compose.

Les instances de préproduction sont utilisées pour les développements, afin de pouvoir garantir le bon fonctionnement des applications lors des mises à jour.

Les applications utilisent Python v3.7 et le framework Django.

Une autre VM (Debian 12 / PostgreSQL) v13 gère les bases de données des instances applicatives. Il y a donc au total 6 bases PostgreSQL.

L'installation Debian/PostgreSQL est standard. (sans Docker sur cette VM). La sécurité est gérée au niveau des accès (distinct pour chaque instance).

La VM d'accès est utilisée pour les accès SSH externes (développement).

La VM OPNSense reçoit le trafic vers les applications sintes-lab, et le dirige sur les applications en fonction de l'URL demandée. Elle fait aussi office de pare-feu si besoin.

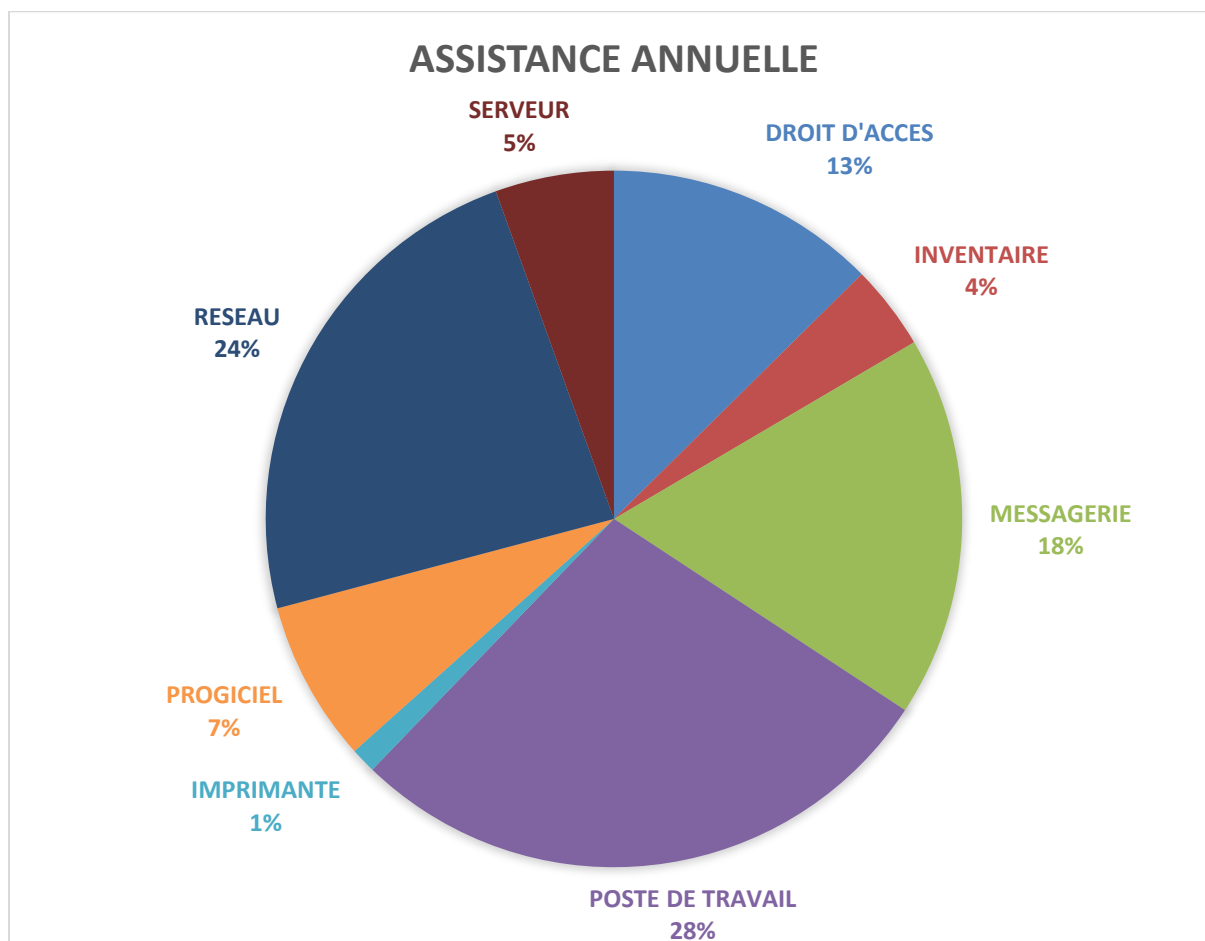
Cette VM n'est pas connectée directement à internet, et le trafic vers les applications et les accès développement lui est envoyé par l'équipement réseau principal (transfert de ports).

Reverse proxy, pour pouvoir distinguer le trafic Sintes du trafic Web et le rediriger vers le bon serveur.

2.13. Helpdesk / Gestion parc

- L'ITSM est géré et hébergé par l'actuel titulaire.

Répartition des demandes de support annuel et exemples.



Catégorie	nb annuel
DROIT D'ACCES	32
INVENTAIRE	10
MESSAGERIE	45
POSTE DE TRAVAIL	71
IMPRIMANTE	3
PROGICIEL	19
RESEAU	60
SERVEUR	14

Quelques exemples :

- Droits d'accès : droits NTFS, partage de document
- Inventaire : Mise à jour inventaire, extraction de date de garantie, rédaction de procédure
- Messagerie : ajout à une liste de diffusion, création de compte
- Poste de travail : installation de logiciel sur un poste, problème matériel, utilisation générale du poste
- Imprimante : installation du copieur réseau sur un poste.

- Progiciels : Mise en œuvre de patch, mise en œuvre certificat SSL, application de procédure fournie par l'éditeur
- Réseau : Problème lié au VPN, connexion internet, réglage proxy. Notez que suite à une migration les tickets réseau sont anormalement élevés. Cette situation est éphémère et dépendra de la stabilité du SI dont le titulaire aura la charge.
- Serveur : mise à jour, paramétrage, diagnostic

2.14. Documentation

Le système d'information est très peu documenté. (inventaire parcellaire, pas de schéma ni de dossier d'exploitation)

Une prestation en début de mission sera commandée afin de compléter la documentation.

2.15. Projets à venir

- Intégration au Réseau Interministériel de l'Etat

Il s'agit d'un réseau MPLS sans accès internet pour le partage d'applicatif au sein des entités de l'Etat.

Les candidats intégreront sans surcoût ce nouveau réseau au sein de l'OFDT. Gestion des interfaces sur le firewall, paramétrage, règle de gestion, matrice de flux.

3. PERIMETRE D'INTERVENTION

Pour permettre aux candidats de définir au mieux le coût du forfait et ses engagements, ci-dessous une liste non exhaustive des tâches attendues.

3.1. Référent technique

3.1.1. Périmètre

Sur sollicitation du maître d'ouvrage, sur l'ensemble des projets. En qualité de référent technique.

3.1.2. Attentes

Conseiller la collectivité dans la mise en œuvre de ses projets en matière d'interopérabilité, d'intégration, de documentation technique.

Être l'intermédiaire du maître d'ouvrage avec l'ensemble de ses prestataires informatiques.

Être force de conseil quant au choix des matériels acquis à travers un autre marché dédié.

3.1.3. Tâche type

- Valider l'intégration au SI
- Relecture des DAT
- Accompagnement le maître d'ouvrage dans l'intégration des nouveaux services
- Appel d'un éditeur métier
- Coordination entre prestataire
- Coordination avec le titulaire du marché de matériel, de téléphonie, d'accès internet

3.2. Postes clients – Assistance utilisateurs

3.2.1. Périmètre

La dénomination postes clients inclue : PC fixes, PC portables, Téléphones portables, Tablettes, imprimantes locales.

3.2.2. Attentes

Le support de premier niveau et l'assistance aux utilisateurs.

Hotline utilisateur.

Installation et/ou remplacement des postes acquis au travers le marché de matériels.

3.2.3. Tâches types

- Assistance technique à distance
- Assistance technique sur site
- Installation nouveaux postes

3.3. Administration système

3.3.1. Périmètre

Sur l'ensemble du périmètre décrit dans le chapitre « existant ».

3.3.2. Attentes

- Veiller à la disponibilité, à la stabilité, à la robustesse et à la performance du SI
- Assurer la maintenance préventive et curative
- Administrer, exploiter et superviser le SI
- Le titulaire devra traiter et répondre aux demandes relatives à l'infrastructure (rajout de serveurs Virtuels, espace disque, entrées DNS...)
- Le titulaire doit répondre aux besoins des projets et également à l'évolution naturelle du SI
- Résolution des incidents de production en respectant les délais de rétablissement

3.3.3. Tâches types

- Rajout de VM
- Redémarrage de services et/ou serveurs
- Traitement des demandes de création/modification/suppression de GPO
- Traitement des demandes de création/modification/suppression des objets de l'AD
- Traitement des tickets de niveau 2 et 3
- Diagnostiquer un dysfonctionnement du SI
- Conseiller le maître d'ouvrage dans le cadre d'un projet
- Mise à jour des droits NTFS
- Création/Application de script système
- Réalisation de bascule de l'infrastructure (Test du PCA...)
- Traitement des demandes de création/modification/suppression DNS et DHCP

3.4. Administration réseau

3.4.1. Périmètre

Sur l'ensemble du périmètre décrit dans le chapitre « existant ».

3.4.2. Attentes

- Veiller à la disponibilité, à la stabilité du réseau
- Assurer la maintenance préventive et curative
- Administrer, exploiter et superviser le réseau
- Paramétrage du firewall
- Le futur titulaire devra traiter et répondre aux demandes relatives au réseau (Intervention physique, modification de ports, etc.)
- Le titulaire pourra répondre aux besoins des projets et également à l'évolution naturelle du réseau
- Résolution des incidents de production en respectant les délais de rétablissement

3.4.3. Tâches types

- Modification d'une configuration réseau (VLAN, Routage statique dynamique, ports...)
- Changement d'un équipement défectueux
- Diagnostiquer une lenteur réseau (LAN, WAN, WIFI...)
- Diagnostiquer un problème de performance réseau (LAN, WAN, WIFI...)

- Déploiement réseau
- Sauvegarde / Restauration des configurations des Switchs

3.5. Mises à jour

3.5.1. Périmètre

Sur l'ensemble du périmètre décrit dans le chapitre « existant ».

3.5.2. Attentes

Être force de proposition quant à l'application des mises à jour nécessaires au maintien en condition opérationnelle et à la garantie de la sécurité du système d'information.

Le titulaire a un devoir d'alertes sur les mises à jour à appliquer. Il doit en faire valider les impacts fonctionnels auprès de la maîtrise d'ouvrage et appliquer les mises à jour le cas échéant.

3.5.3. Tâches types

- Assurer une vigilance sur les mises à jour à appliquer
- Planifier les mises à jour et obtenir les approbations nécessaires
- Définir le plan d'implémentation (test, préprod et prod selon les périmètres)
- Application des mises à jour

3.6. Sauvegarde

3.6.1. Périmètre

Sur l'ensemble du périmètre décrit dans le chapitre « existant »

3.6.2. Attentes

- Connaître les exigences du RGPD en matière de sauvegarde et d'archivage des données à caractère personnel
- Le futur titulaire devra veiller à la bonne exécution des sauvegardes
- S'assurer de la fiabilité des sauvegardes
- Garantir la sauvegarde de l'ensemble du périmètre

3.6.3. Tâches types

- Restauration (sur demande / test de bon fonctionnement)
- Vérification des sauvegardes
- Restauration VM, granulaire (mail, fichier etc....)
- Mise à jour du logiciel de sauvegarde TEST et PROD
- Traitement des erreurs de sauvegarde
- Ajouter les nouvelles VM dans le processus de sauvegarde de façon systématique
- Test de sauvegarde et de restauration

3.7. Anti-Virus et sécurité

3.7.1. Périmètre

Sur l'ensemble du périmètre décrit dans le chapitre « existant ».

3.7.2. Attentes

- Le futur titulaire devra veiller à ce que les signatures soient à jour

3.7.3. Tâches types

- Mise à jour des antivirus
- Extraction de logs pour analyse
- Traitement des alertes de sécurité
- Traitement des demandes de modification, création des règles de sécurité (FW, WAF et PROXY...)
- Traitements des demandes de modification, création des entrées dans l'antispam
- Traitements des demandes de modification, création des certificats

3.8. Applicatifs

3.8.1. Périmètre

L'infogérant a la charge de l'exploitation de l'environnement technique (On Premise) sur lequel repose les logiciels du maître d'ouvrage.

3.8.2. Attentes

- Administration des serveurs (infrastructure et web)
- Gestion des accès externes
- En cas de difficultés particulière prendre en charge la demande et faire le lien avec l'éditeur métier

3.8.3. Tâches types

- Mise en œuvre et administration d'un reverse proxy
- Appel de l'éditeur (relais technique de la collectivité)
- Mise en œuvre de certificat SSL
- Redémarrage de serveur
- Mise en œuvre de procédure fournie par les éditeurs (mise à jour de version, patch..)
- Déploiement d'infrastructure pour un projet applicatif

3.9. Messagerie

3.9.1. Périmètre

Sur l'ensemble du périmètre décrit dans le chapitre « existant ».

3.9.2. Attentes

- Veiller à la disponibilité, à la stabilité de la messagerie

- Assurer la maintenance préventive et curative
- Administrer, exploiter et superviser la messagerie
- Résolution des incidents de production en respectant les délais de rétablissement
- Administration exchange

3.9.3. Tâches types

- Diagnostiquer les incidents techniques
- Tracking des mails

3.10. Supervision

3.10.1. Périmètre

Sur l'ensemble du périmètre décrit dans le chapitre « existant ».

La supervision s'exerce au travers d'un outil proposé et mis en œuvre par le titulaire.

Administration de la solution de supervision

Il est attendu de l'infogérant la réalisation de contrôle quotidien du bon fonctionnement du système d'information.

3.10.2. Attentes

- Détection des incidents
- Déclenchement des actions correctrices lors des alertes et respecter les temps de résolution des incidents
- Force de proposition sur l'évolution de la supervision
- Maintien en condition opérationnelle de la solution de supervision (mise à jour...)
- Réalisation, suivi et envoi des tableaux de bord du SI (quotidien)

3.10.3. Tâches types

- Ajout de sonde ou points de vérification
- Traitement des alertes
- Mise à jour de version
- Réalisation de rapports avec des scripts ou les outils du département
- Ajouter les sondes suite à un ajout de matériel, logiciel, application...
- Reporting technique
- Réalisation des tableaux de bord du SI
- Réalisation d'analyses ponctuelles sur un équipement, service...

3.11. Documentation

3.11.1. Périmètre

Sur l'ensemble de son périmètre d'intervention la création et la mise à jour de toute la documentation standard et technique, ainsi que la mise à jour de la documentation (DEX, DAT...etc.). Cette

documentation devra être rédigée dans un souci de transfert de compétence (donc suffisamment détaillée).

3.11.2. Attentes

Complétion de la documentation existante.

- Documenter systématiquement les procédures appliquées
- La documentation doit être mise à jour au plus tard sous 3 semaines après une mise en œuvre
- Réalisation de documentation d'architecture

3.11.3. Tâches types

- Rédaction et mise à jour de la documentation et des procédures
- Rédaction et mise à jour des plans d'infrastructure
- Réalisation de tâche d'administration avec le technicien interne
- Rédaction et mise à jour de la politique de sauvegarde
- Rédaction et mise à jour de procédures liées à la reprise et continuité d'activité

4. GOUVERNANCE

4.1. Suivi des interventions - ITSM

Le candidat proposera un outil de ticketing au travers lequel les demandes pourront être suivies. Le représentant du maître d'ouvrage doit avoir un accès complet à la base incident afin de pouvoir en avoir une vue globale. Les candidats préciseront dans leur mémoire technique les modalités d'utilisation de leur plateforme de suivi des demandes.

4.2. Inventaire - ITSM

L'inventaire des actifs devra être tenu à jour par le titulaire.

Celui-ci devra intégrer des éléments permettant une gouvernance du plan de renouvellement (date d'achat, fournisseur, mise en service, durée garantie, coût unitaire, utilisateur associé, modèle, numéro de série, lieu, état...).

Le maître d'ouvrage pourra demander régulièrement des exportations de cette base. Notamment pour lui permettre d'organiser le renouvellement du parc.

Le titulaire mettra à disposition du maître d'ouvrage un accès complet à l'ITSM. Accès utilisateur pour le suivi de ses tickets, chef de service pour la supervision des demandes d'un groupe d'agent, administrateur permettra la consultation de l'ensemble des éléments composant le parc.

Le titulaire pourra solliciter la collectivité pour compléter les éléments liés à la gestion administrative (coût, numéro bon de commande, date d'achat etc.).

4.3. Interlocuteur privilégié

Il est demandé expressément aux candidats de désigner une personne unique en charge du suivi global de la prestation.

Celle-ci sera garante du niveau de prestation globale et pourra être joignable directement par le maître d'ouvrage pour toutes questions concernant le suivi du marché.

C'est cet interlocuteur privilégié qui sera en charge des rapports d'activité et comité de pilotage.

Il est expressément demandé que cet interlocuteur soit un opérationnel intervenant régulièrement sur l'infrastructure de la collectivité (par exemple un administrateur système référent).

4.4. Rapport d'activité

Fréquence

Tous les 3 mois.

Modalité

Envoi d'un récapitulatif de l'activité trimestrielle :

- Nombre de demande de support ouvert / résolu
- Tâche relevant de l'administration système réalisée / planifiée / à programmer

Ces rapports ont pour objectif de permettre au maitre d'ouvrage d'avoir une vue objective des actions mises en œuvre.

Livrable

Rapport d'activité

4.5. Comité de pilotage

Fréquence

Tous les 3 mois.

Participants

Interlocuteur privilégié accompagné éventuellement du responsable commercial et/ou technique, représentants du maitre d'ouvrage.

Modalité

Animé par le titulaire ces revues auront pour objectif de donner une vision globale de son système d'information au maitre d'ouvrage. Le titulaire présente les actions structurantes menées et à venir concernant le maintien en condition opérationnel du système d'information et son évolution.

Peut être proposée sur site ou en visio.

Livrable

Compte rendu.

Celle-ci doit donner lieu, le cas échéant à un plan d'action.

5. ENGAGEMENTS CONTRACTUELS

5.1. Plage de service garanti (PSG)

Du lundi au vendredi de 8h00 à 17h00.

5.2. Garantie de Temps de Rétablissement

La GTR ne s'applique que durant la Plage de Service Garanti (PSG).

Les candidats sont invités à proposer une GTR qui leur paraît la plus adaptée en respectant une durée maximum précisée ci-après (pendant la PSG).

Les délais se calculent en heures sur la plage de service garanti.

5.3. Définition des niveaux de criticité

Niveau	Description	GTR maximum
Critique	Impactant plus de 50 % des utilisateurs ou Messagerie hors service ou Contrôleur hors service ou Serveur de fichier ou applicatif hors service	4h
Bloquant	Rendant impossible la réalisation de mission liée au service public.	8h
Mineure	Impactant moins de 20% des agents Sans incidence sur les missions de service public	12h

5.4. Accès

Le titulaire mettra à disposition du maître d'ouvrage une base de données intégrant l'ensemble des accès qu'il détient au système d'information et notamment ceux à privilèges (système, réseau, applicatif).

Celle-ci devra être tenue à jour tout au long du marché.

5.5. Fin de contrat

A la fin du présent marché, en cas de changement de titulaire, le titulaire actuel mettra à disposition du nouvel attributaire un interlocuteur en capacité de présenter l'ensemble du système d'information et de fournir le dossier de site complet (inventaire, plan, schéma, accès).

Modalité : 1 journée de présence sur site à fixer en accord avec le maître d'ouvrage.

6. MODALITE D'INTERVENTION

6.1. Déplacements

Les déplacements seront très limités, la prestation s'effectuant uniquement sur les sites précisés en début de document.

6.2. Intervention sur site / distante

Les candidats préciseront dans leur mémoire technique les modalités d'intervention sur site et/ou distante. (passage récurrent, limites, délais d'intervention...)

7. PARTIE FORFAITAIRE (DPGF)

7.1. Coût infogérance

Le coût mensuel et forfaitaire de la prestation d'infogérance dans sa globalité, frais inclus.

Il est attendu un coût forfaitaire ne variant pas en fonction des entrées – sorties d'agents.

Il n'est pas prévu de forte variation (+/-) 20 agents sur la durée du marché.

Conscient que la difficulté du chiffrage de ce type de prestation est dépendante de la précision du périmètre et des attentes quelques éléments :

- Volontairement, le maître d'ouvrage ne définit pas la volumétrie de la prestation d'infogérance attendue. (Nombre de jour, présence sur site, nombre et type de profil dédié...)
- L'évaluation du nombre de jour nécessaire sur site / à distance est à estimer vis-à-vis de l'expérience acquise chez d'autres clients. (À préciser dans le mémoire technique)
- L'analyse des offres tenant compte du prix mais également du contenu des prestations un juste équilibre est à trouver.
- Afin de proposer un coût récurrent le plus juste possible, il est proposé aux candidats de fixer (ou non) une limite de prestation. Celle-ci sera évaluée au travers un critère de jugement des offres. Un juste équilibre est à trouver pour optimiser votre offre.
- C'est une des raisons pour laquelle un BPU est adossé à l'offre forfaitaire.

Les attentes peuvent paraître importantes mais il s'agit en réalité de tâches assez classiques d'un contrat d'infogérance pour un système d'information de taille très réduite.

Tenez en compte en évaluant le coût mensuel.

Les éventuelles limites de prestation proposées par les candidats sont à préciser dans l'acte d'engagement.

8. BORDEREAU DES PRIX UNITAIRES

Ce chapitre décrit les lignes listées dans l'onglet BPU. (À compléter par les candidats)

8.1. Prix unitaires additionnels

Le BPU ne pouvant être exhaustif au vu de la multiplicité des références matériels, licences, de l'organisation commerciale des différents candidats, il est proposé aux candidats d'ajouter des prix unitaires leur semblant pertinent au vu de la compréhension du besoin dans la section prix additionnels.

Sans caractère obligatoire quelques exemples :

- NAS de différentes capacités
- Licences logicielles
- Bornes wifi
- Prestation spécifique
- ...

8.2. Initialisation de la mission

Il vous est demandé de chiffrer un coût forfaitaire d'initialisation de la mission.

Ceci a pour but d'éviter aux candidats de devoir lisser mensuellement le surcoût de début de prise en charge.

Cette initialisation doit intégrer :

- La prise en compte de l'existant
- La passation avec l'actuel titulaire
- La production d'une note dite « d'étonnement » (présentation de constats, de préconisations, difficultés liées à la prise de fonction).
- [PRA] La production d'un plan d'action (note de synthèse) permettant une reprise d'activité sur un risque de CryptoLocker touchant les VM et stockages non spécifiquement protégés. Si des actions préalables devaient être prise afin de rendre possible ce plan d'action elles devront être précisées dans celui-ci. La prestation éventuelle pourra dans ce cas être commandée dans le cadre du BPU. Le cas échéant, matériel et logiciel spécifique seront commandés dans le cadre de prestation similaire. Il ne s'agit d'intégrer au coût de la prestation d'initialisation **que la rédaction** de cette note et aucune prestation ou fourniture de matériels ou licence.

Le titulaire dispose de 3 mois à l'issue de la notification du bon de commande pour mettre en œuvre cette prestation d'initialisation.

8.3. Sauvegarde externalisée

Comprend la sauvegarde de l'ensemble des VM pour un volume total de 4 To.

8.4. Licences

8.4.1. Licence antivirus poste client

Intégrant a minima

- Antivirus
- Analyse des appareils externes
- Intégré au sein d'une console de supervision

8.4.2. Constitution dossier de site

Réalisation de l'inventaire exhaustif du parc informatique (modèle, spécification technique, date d'achat, garantie en cours...).

Réalisation de schéma d'infrastructure.

Réalisation schéma réseau.

8.4.3. Licence antivirus serveur

Peut être identique à ce qui est proposé pour le poste client

Intégrant a minima

- Antivirus et firewall
- Analyse des appareils externes
- Intégré au sein d'une console de supervision

8.5. Profils

Une même personne peut cumuler les compétences de différents profils. Les différents profils doivent intégrer une bonne connaissance du RGPD.

8.5.1. Technicien

- Expérience de 2 ans minimum
- Bac minimum
- Application des mises à jour
- Installation et configuration des ressources matérielles documentées
- Suivi du parc informatique
- Assistance utilisateur

8.5.2. Administrateur système junior

- Expérience de 2 ans minimum
- Bac + 2 minimum
- Administrateur Windows serveur
- Administration Linux
- Application des mises à jour
- Mise à jour de la documentation

- Installation et configuration des ressources matérielles
- Procédure et règles d'utilisation
- Administrer les annuaires LDAP
- Suivi du parc informatique
- Veille Technologique
- Gestion des incidents
- Assistance utilisateur
- Assistance et conseil utilisateur

8.5.3. Administrateur système senior

- Expérience de 5 ans minimum
- Formation Bac + 3 minimum
- Administrateur Windows serveur
- Administration Linux
- Application de GPO
- Application des mises à jour
- Mise à jour de la documentation
- Sécurité et maintenance des données
- Sauvegarde et restauration des systèmes de bases de données
- Superviser les ressources systèmes
- Constituer des dossiers d'architectures et intervenir auprès de différents clients en tant que référent technique
- Réagir aux inefficiences du système et résoudre rapidement les problèmes afin d'assurer sa disponibilité et sa performance en niveau de support N3
- Définir l'architecture globale des systèmes d'information et les conditions de maintenance
- Participer à la construction d'architectures du SI ainsi qu'à la définition des préconisations
- Anticiper les évolutions des TIC techniques, juridiques et réglementaires et leurs impacts sur les SI
- Définir et mettre en place les outils de supervision, normalisation, d'automatisation et de sécurisation de la production.
- Assurer et optimiser l'industrialisation de la production.
- Réaliser l'analyse des contraintes d'exploitabilité.
- Participer, en amont, à la création, intégration et déploiement de solutions applicatives.
- Procédure et règles d'utilisation
- Administrer les annuaires LDAP
- Mettre en place une politique des droits d'accès
- Suivi du parc informatique
- Gestion des incidents
- Expertise virtualisation
- Veille Technologique

8.5.4. Administrateur réseau

- Assurer l'installation des infrastructures réseau en suivant les procédures fournies par le maître d'ouvrage
- Garantir les performances des équipements réseau
- Contrôler le bon fonctionnement des matériels pour garantir la fiabilité du réseau
- Organiser et réaliser les opérations de maintenance et d'entretien pour réduire les pannes techniques
- Organiser et réaliser les mises à jour des équipements réseau
- Avoir une connaissance approfondie des technologies et des équipements réseau
- Maîtriser les protocoles de communication et de sécurité informatiques
- Très bonne connaissance des protocoles de réseaux : TCP/IP, Ethernet, LAN, WAN...
- Bonne connaissance des systèmes d'exploitation, serveur de messagerie
- Très bonnes connaissances des technologies de télécommunication et internet : DNS, SSH, FTP, DHCP...
- Bonne connaissance en cybersécurité : Firewall, antivirus, serveurs d'authentification...
- Très bonne connaissance des Switchs, firewall, routage...

8.5.5. Chef de projet

- Piloter l'avancement des projets, suivre les charges et les indicateurs associés, et coordonner l'ensemble des parties prenantes,
- Être garant de la relation entre les parties prenantes
- Assurer le reporting à la collectivité, intégrant les volets risques et alertes
- Estimer les moyens nécessaires, évaluer les coûts et le budget
- Capacité de rédaction et de présentation
- Aisance orale

8.5.6. Câblage

Disposant des habilitations permettant

- Brassage de baie informatique
- Refonte baie de brassage
- Pose de prise réseau
- Pose de prise électrique
- Travail en hauteur (<5m)