

EPMS DE L'OURCQ

CAHIER DES CLAUSES TECHNIQUES PARTICULIERES

Migration vers l'écosystème Microsoft 365 et Azure et Infogérance

MARCHE A PROCEDURE ADAPTEE

La procédure est passée en application des dispositions des articles R 2123-1 et R 2123-4 du code de la commande publique (Décret n°2018-1075 du 3 décembre 2018 portant partie réglementaire du code de la commande publique)

ACCORD-CADRE

MARCHE A BONS DE COMMANDE

Pouvoir adjudicateur

EPMS de l'Ourcq
Représentée par Mme OUMOU KEÏTA, directrice
Allée André Benoist
77410 CLAYE SOUILLY

DATE LIMITE DE REMISE DES OFFRES : 30 septembre 2026 à 18h00

Termes	Définition
Accès Conditionnel	Fonctionnalité de Microsoft Entra ID permettant d'appliquer des règles de sécurité (ex: exiger le MFA) en fonction du contexte de connexion (lieu, terminal, etc.).
AMOA	Assistance à Maîtrise d'Ouvrage
AVD	Azure Virtual Desktop
CCTP	Cahier des Clauses Techniques Particulières
DAT	(Document d'Architecture Technique) Livrable clé décrivant la conception de la solution cible.
DEX	(Dossier d'Exploitation) Livrable clé décrivant comment administrer la solution livrée.
DLP	(Data Loss Prevention) Prévention de la Perte de Données. Politiques visant à empêcher la fuite d'informations sensibles.
DPO	(Data Protection Officer) Délégué à la Protection des Données. Garant de la conformité RGPD.
EDR	Endpoint Detection and Response
Entra ID	Microsoft Entra ID (anciennement Azure Active Directory)
Exchange Online	Service de messagerie et de calendrier de la suite Microsoft 365 (partie Cloud).
Fichiers partagés	Répertoires réseaux, serveurs de fichiers
FSLogix	Technologie utilisée pour gérer les profils utilisateurs dans les environnements de bureau virtuel (comme AVD).
GTI	(Garantie de Temps d'Intervention) Délai contractuel dans lequel l'infogérant s'engage à commencer à traiter un incident.
GTR	(Garantie de Temps de Rétablissement) Délai contractuel dans lequel l'infogérant s'engage à résoudre un incident.
HDS	Hébergeur de Données de Santé
IaaS	(Infrastructure as a Service) Modèle de cloud où l'on loue l'infrastructure de base (VM, stockage, réseau).
ITIL	(Information Technology Infrastructure Library) Ensemble de bonnes pratiques pour la gestion des services informatiques (gestion des incidents, des problèmes, etc.).
MCO	Maintien en Condition Opérationnelle
MFA	Multi-Factor Authentication
MS365	Microsoft 365
OneDrive Entreprise	Espace de stockage de fichiers individuel dans le cloud Microsoft 365.
PaaS	(Platform as a Service) Modèle de cloud où l'on loue une plateforme applicative (ex: base de données) sans gérer les serveurs sous-jacents.
PAQ	(Plan d'Assurance Qualité) Livrable décrivant l'organisation et les méthodes du titulaire pour garantir la qualité du projet.
PGSSI-S	Politique Générale de Sécurité des Systèmes d'Information de Santé. Cadre réglementaire de sécurité s'appliquant à l'EPMS.
PRA / PCA	Plan de Reprise d'Activité / Plan de Continuité d'Activité
PST	(Personal Storage Table) Fichier d'archive personnel pour les emails Outlook (souvent stocké localement ou sur un serveur de fichiers).
RDS	(Remote Desktop Services) Solution Microsoft On-Premise permettant de fournir des bureaux ou des applications à distance (l'existant).
RSE	(Responsabilité Sociétale des Entreprises) Prise en compte des enjeux sociaux et environnementaux dans l'activité de l'entreprise.
RSSI	Responsable de la Sécurité des Systèmes d'Information
RTO / RPO	Recovery Time Objective / Recovery Point Objective
SaaS	(Software as a Service) Modèle de cloud où l'on loue une application clé en main (ex: Microsoft 365).
SharePoint Online	Service de gestion de contenu et de collaboration (sites d'équipe, intranets, gestion documentaire) de la suite Microsoft 365.

SLA	Service Level Agreement (Accord de Niveau de Service)
SSO	Single Sign-On
Teams	Plateforme de communication et de collaboration de Microsoft 365 (messagerie instantanée, visioconférence, équipes).
TF	(Tranche Ferme) Partie du marché que l'acheteur s'engage à commander.
TO	(Tranche Optionnelle) Partie du marché que l'acheteur se réserve le droit de commander ou non.
UAT	User Acceptance Testing (Tests d'Acceptation Utilisateur)
UPN	User Principal Name
VABF	(Vérification d'Aptitude au Bon Fonctionnement) Phase de tests internes du titulaire.
VPN	(Virtual Private Network) Réseau privé virtuel, utilisé pour créer un tunnel sécurisé (ex: entre le site client et Azure).
VSR	(Vérification de Service Régulier) Phase de tests et de recette menée par le client.

Glossaire des Termes & Abréviations

Table des matières

Partie 1 : Tronc commun (Applicable aux lots 1 et 2).....	8
1 Introduction.....	8
1.1 Objet du marché	8
1.2 Objet du document (CCTP).....	9
2 Présentation de l'EPMS de l'OURCQ	9
2.1 Présentation générale	9
2.1.1 Statut et mission principale	9
2.1.2 Organisation et établissements	10
2.1.3 Enjeux et contexte du projet.....	10
2.2 Briques du futur système d'informations.....	11
2.3 Vue d'ensemble de l'architecture actuelle	12
2.3.1 Infrastructure réseau et connectivité	12
2.3.2 Réseau local (LAN) et segmentation	13
2.3.3 Annuaire Active Directory	14
2.3.4 Messagerie actuelle	15
2.3.5 Serveurs de fichiers et gestion documentaire.....	16
2.3.6 Environnement bureautique et postes de travail.....	16
2.3.7 Applications métiers	17
2.3.8 Impression	18
2.3.9 Profils utilisateurs et spécificités d'usage	18
2.3.10 Contexte d'utilisation et d'accompagnement	19
2.4 Sécurité actuelle et conformité	19
2.4.1 Cadre réglementaire et légal	19
2.4.2 Mesures de protection des données actuelles.....	20
2.4.3 Usages et circulation des données de santé	20
3 Exigences fonctionnelles transverses	21
3.1 Exigences générales (Collaboration, Mobilité, Productivité)	21
3.2 Exigences spécifiques à la messagerie.....	21
3.3 Exigences spécifiques aux fichiers & à la gestion documentaire	22
3.4 Exigences spécifiques à la communication & visioconférence	22

3.5	Exigences spécifiques au bureau à distance	22
3.6	Exigences liées aux applications métiers	23
3.7	Sécurité et conformité	23
3.8	Performance et disponibilité	24
3.9	Gouvernance et opérabilité	24
4	Exigences en matière de Responsabilité Sociétale et Environnementale (RSE)	25
4.1	Volet environnemental ("Numérique responsable")	25
4.2	Volet social et sociétal	25
Partie 2 : Spécifications du Lot 1 - Fourniture des licences Microsoft 365, prestation de migration technique & accompagnement des utilisateurs au changement.....		
5	Description et périmètre du Lot 1	26
5.1	Objectifs spécifiques du Lot 1	26
5.2	Périmètre des prestations attendues	27
5.2.1	Fourniture des licences	27
5.2.2	Fourniture et configuration de l'infrastructure réseau	27
5.2.3	Prestations de migration technique et d'infrastructure	27
5.2.4	Prestations d'accompagnement au changement et de formation	28
6	Exigences techniques de la solution cible (Lot 1)	29
6.1	Exigences d'architecture générale.....	29
6.2	Exigences pour la fourniture des licences Microsoft 365	29
6.3	Exigences de gestion des identités et des accès (Entra ID)	30
6.4	Exigences pour le service de messagerie	31
6.5	Exigences pour la collaboration et les fichiers (SharePoint / OneDrive / Teams).....	32
6.6	Exigences pour le bureau à distance (Azure Virtual Desktop)	33
6.7	Exigences pour la solution de sécurité des terminaux (Antivirus / EDR).....	34
6.8	Exigences pour le remplacement des pare-feux locaux.....	35
6.9	Exigences pour les interconnexions (VPN)	35
6.10	Exigences pour la solution d'impression sécurisée	36
6.10.1	Choix technologique et architecture générale	36
6.10.2	Infrastructure technique – VM d'impression.....	36
6.10.3	Déploiement des imprimantes et configuration GPO	37
6.10.4	Coordination avec GESPAGE :	37

6.11	Exigences transverses de sécurité	37
6.12	Exigences d'administration et d'exploitation	38
7	Exigences d'accompagnement au changement et formation	40
7.1	Stratégie et planification	40
7.2	Communication	40
7.3	Ingénierie pédagogique et formation	41
7.4	Support post-migration	41
8	Méthodologie et livrables Attendus pour le Lot 1	42
8.1	Gouvernance et gestion de projet	42
8.2	Livrables attendus	42
8.3	Exigences de tests et recette	43
8.4	Transfert de compétences	44
Partie 3, dédiée au Lot 2 : Infogérance		45
9	Description et Périmètre du Lot 2	45
9.1	Objectifs Spécifiques du Lot 2	45
9.2	Périmètre des Prestations Attendues	45
9.2.1	Tranche Ferme (Obligatoire) : Infogérance de l'Écosystème Cloud	45
9.2.2	Tranche Optionnelle (Facultative) : Infogérance du Parc Local	46
9.3	Livrables et Interface Lot 1 → Lot 2	47
10	Exigences pour les Prestations d'Infogérance (Lot 2)	49
10.1	Exigences d'Administration et d'Exploitation des Services M365	49
10.2	Exigences de Support aux Utilisateurs (Centre de Services)	49
10.3	Exigences d'Administration et d'Exploitation des Services Azure	50
10.4	Exigences de Supervision et de Sécurité	51
10.5	Exigences de Mise en œuvre et d'exploitation de la sauvegarde	52
10.5.1	Conception et mise en œuvre	52
10.5.2	Exigences Fonctionnelles et de Rétention	52
10.5.3	Exigences d'exploitation quotidienne	52
10.6	Exigences d'Administration et d'Infogérance des Firewall	53
10.6.1	Supervision et Monitoring	53
10.6.2	Maintien en Condition Opérationnelle (MCO)	53
10.6.3	Gestion des Incidents de Sécurité Réseau :	54

10.6.4	Engagements de Service (SLA)	54
10.6.5	Intégration aux Processus de Gouvernance	55
10.7	Exigences de pilotage, qualité de service et comitologie	55
10.7.1	10.6.1 Définition des niveaux de priorité	55
10.7.2	10.6.2 Engagements de niveaux de service	55
10.7.3	10.6.3 Gouvernance et suivi de service	56
10.7.4	10.6.4 Rapports d'activité	56
10.8	Exigences relatives à la tranche optionnelle (parc local)	57
11	Réversibilité	58
11.1	Objet de la réversibilité	58
11.2	Obligations du titulaire	58
11.3	Modalités de mise en œuvre	58
11.4	Garanties et pénalités	59
11.5	Confidentialité et sécurité	59

Partie 1 : Tronc commun (Applicable aux lots 1 et 2)

1 Introduction

1.1 Objet du marché

Le présent marché a pour objet la modernisation du système d'information de l'EPMS de l'Ourcq. La prestation consiste en la migration de l'infrastructure et des services existants (messagerie, serveurs de fichiers, bureaux à distance) vers l'écosystème cloud de Microsoft (Microsoft 365 et Microsoft Azure). L'objectif est de doter l'établissement d'une solution performante, évolutive et sécurisée, tout en garantissant la conformité avec la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) à laquelle est soumise l'EPMS.

L'EPMS de l'Ourcq connaît actuellement une situation d'urgence technique documentée avec un coût de maintien en vie représentant 65% du budget informatique sans création de valeur opérationnelle.

Le présent marché vise donc à :

- **Reconstruire sur de nouvelles fondations** une infrastructure pérenne, sécurisée et performante.
- **Répondre aux enjeux opérationnels** documentés lors de la tenue d'ateliers d'expression d'utilisateurs sur les aspects : collaboration, mobilité, gestion documentaire, communication structurée.
- **Garantir la conformité réglementaire avec la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S), HDS, Règlement Général** sur la Protection des Données et autres exigences médico-sociales.
- **Assurer l'adoption durable** par un accompagnement au changement adapté à un personnel peu familier avec les technologies informatiques.
- **Sécuriser les données de santé** en transit et au repos, avec des mécanismes de contrôle et de traçabilité conformes aux obligations légales.

Ce marché est décomposé en **deux lots distincts** :

- **Lot 1 : Fourniture des licences, Fourniture et Paramétrage de Firewall, Prestation de migration technique et Accompagnement au changement.**
Ce lot couvre la fourniture des abonnements, la réalisation du projet de migration technique vers le cloud, ainsi que l'intégralité du volet humain (communication, formation et accompagnement des utilisateurs).

- **Lot 2 : Infogérance de l'écosystème.** Ce lot couvre l'exploitation, la supervision, la sauvegarde, la sécurité et le support de la nouvelle plateforme cloud (Tranche Ferme), ainsi qu'une option pour l'infogérance du parc local (Tranche Optionnelle).

1.2 Objet du document (CCTP)

Le présent document constitue le Cahier des Clauses Techniques Particulières (CCTP) du marché relatif à la migration de l'environnement de travail numérique de l'EPMS vers l'écosystème Microsoft 365 et aux prestations associées. Il définit :

- Le contexte et l'environnement technique existant (infrastructure actuelle, enjeux, urgence).
- Les exigences fonctionnelles, techniques et de sécurité de la solution cible.
- La méthodologie de projet attendue pour les prestations de migration.
- Les prestations d'accompagnement au changement et de formation.
- Les niveaux de service attendus pour le support et le maintien en condition opérationnelle.
- Les conditions de recette et d'acceptabilité des livrables.

Le candidat devra répondre de manière exhaustive à l'ensemble des exigences formulées dans le présent document. Les réponses devront être formalisées dans son mémoire technique ainsi que dans l'**Annexe X – Cadre de Réponse Technique** jointe au dossier de consultation.

Le mémoire technique et les réponses apportées dans cette annexe auront valeur contractuelle.

2 Présentation de l'EPMS de l'OURCQ

2.1 Présentation générale

2.1.1 Statut et mission principale

L'Établissement Public Médico-Social de l'OURCQ accompagne des personnes enfants, adolescents et jeunes adultes de 0 à 20 ans et présentant des troubles du neurodéveloppement.

L'EPMS de l'OURCQ relève de la fonction publique hospitalière. En tant qu'établissement médico-social, l'EPMS est obligatoirement soumis à la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) et à la certification Hébergeur de Données de Santé (HDS) pour tout système hébergeant ou traitant des données sensibles de santé.

2.1.2 Organisation et établissements

L'EPMS de l'Ourcq s'organise autour de 8 sites géographiques distincts, regroupant différents dispositifs (191 agents) :

- Services éducatifs (unités de vie, activités éducatives).
- Services médicaux et infirmiers (suivi médical, soins).
- Unités d'Évaluation Médico-Sociale (UEMA).
- Services de Manutention Spécialisée (MASCO).
- Pôle administratif (direction, finances, ressources humaines, gestion administrative).

Cette organisation multisite et multi-dispositif est un paramètre clé pour la stratégie de migration : les migrations devront s'effectuer par vagues respectant les frontières organisationnelles.

Il est important de noter que l'EPMS est actuellement en phase de réorganisation logique et physique des sites, que des regroupements vont être effectués et que d'ici fin décembre 2026-Début janvier 2027, seuls 5 sites subsisteront (documentés en section 2.3.1).

2.1.3 Enjeux et contexte du projet

Urgence technique — Faillite documentée

L'infrastructure informatique actuelle de l'EPMS est en situation de défaillance structurelle irréversible : les serveurs critiques fonctionnent sur des versions hors support depuis 2020-2023, sans redondance opérationnelle, sans plan de reprise d'activité.

État des serveurs critiques :

- **Serveur de contrôle de domaine** : Système d'exploitation hors support depuis 2020, concentrant tous les rôles critiques (authentification, annuaire, messagerie).
- **Serveur d'accès distant** : Système d'exploitation hors support depuis 2023, assurant les accès distants à infrastructure de bureau virtuel.
- **Serveur « secondaire »** : ne communique plus correctement avec le contrôleur de domaine en place créant un point de défaillance unique sur le rôle Active Directory.

Conséquences opérationnelles :

- **Point de défaillance unique absolu** : la perte du serveur principal entraînerait un arrêt total de l'authentification pour l'intégralité des agents.
- **Aucun plan de reprise d'activité documenté.**
- **Absence totale de résilience opérationnelle.**
- **Coût du statu quo** : le maintien en vie sans évolution fonctionnelle représente 65% du budget informatique annuel sans création de valeur.

Enjeux opérationnels — Dysfonctionnements documentés

Quatre ateliers utilisateurs conduits en janvier 2026 ont permis de documenter les dysfonctionnements opérationnels majeurs :

- **Matériel & support** : Lenteurs serveur d'accès distant critiques, pénurie de postes informatiques, impossibilité d'utiliser des tablettes ou des appareils mobiles pour le travail terrain, support utilisateurs limité aux heures de bureau. L'ouverture d'un ticket via l'interface WEB uniquement est considérée comme rédhibitoire pour la majorité des utilisateurs.
- **Collaboration & communication** : en l'absence d'outils de messagerie instantanée et de collaboration institutionnels, les agents utilisent des applications grand public (WhatsApp par exemple) pour des communications professionnelles, des données métiers sont potentiellement exposées sur des canaux non sécurisés, il existe une absence de structure par équipes de travail.
- **Gestion documentaire** : Arborescences partagées figées, absence de gestionnaire documentaire, partage par messagerie ou clé USB, documents dupliqués non versionnés, risques de perte et non-conformité archivage légal.
- **Mobilité & accès distants** : Zéro infrastructure sans fil sur les 5 sites, serveur d'accès distant instable et interrompu, accès distants quasi impossibles pour le travail terrain, forfaits mobiles insuffisants pour opérations extérieures (certains collaborateurs intégralement sur site distant n'appartenant pas à l'EPMS doivent utiliser le partage de connexion mobile).

2.2 Briques du futur système d'informations

Avant de moderniser son Système d'Information, l'EPMS a fait réaliser une démarche complète d'étude et de consultation auprès de ses équipes :

- **Phase 1**: Quatre ateliers utilisateurs regroupant l'ensemble des profils métier (matériel & support, collaboration & communication, gestion documentaire, mobilité & accès distants)

- **Phase 2** : Étude d'opportunité (dimensionnement technique, analyse fonctionnelle, évaluation économique)
- **Phase 3** : Analyse comparative des solutions cibles
- **Phase 4** : Analyse coût-bénéfice
- **Phase 5** : Étude des principes de migration

Cette démarche a conclu que l'infrastructure existante ne peut être maintenue et qu'une reconstruction complète s'impose.

Suite aux études d'opportunité et comparatives menées par l'EPMS, l'établissement a acté le choix stratégique de standardiser son environnement de travail sur les technologies Microsoft 365, Azure et GESPAGE. Les prestations du présent marché consistent exclusivement en la configuration, la migration et l'infogérance de cet écosystème cible

2.3 Vue d'ensemble de l'architecture actuelle

L'architecture du Système d'Information de l'EPMS est entièrement centralisée et externalisée. L'infrastructure serveur de l'EPMS repose sur une architecture virtualisée à laquelle l'ensemble des sites géographiques sont interconnectés via des tunnels VPN IPSec.

Cette architecture centralisée crée un point d'accès unique pour tous les sites. Aucun maillage réseau direct entre sites distants n'existe. Il n'y a pas de nécessité à ce que les sites communiquent directement entre eux.

2.3.1 Infrastructure réseau et connectivité

L'infrastructure serveurs est entièrement hébergée sur la plateforme vCloud du prestataire actuel. Les serveurs sont configurés au sein d'un même Vlan. Aucune zone démilitarisée (DMZ) virtuelle n'existe, et aucune isolation n'est mise en place entre le trafic administratif, applicatif et celui des données sensibles.

La supervision de l'infrastructure est assurée par l'outil PRTG, et est strictement limitée aux machines virtuelles du datacenter. Il n'existe aucune visibilité sur le trafic inter-sites ou sur les performances des tunnels VPN IPSec reliant les sites EPMS au datacenter.

Composant	Configuration Actuelle	Remarque
Hébergement serveurs	Plateforme vCloud Heliaq	Entièrement virtualisé, aucun serveur physique sur site
Interconnexion sites	Tunnels VPN IPSec vers le datacenter	Architecture étoile, point d'accès unique
Pares-feux sites	FortiGate (60F au siège, 40F sur les 7 autres sites)	Firewall en SAAS infogérés par l'hébergeur actuel.
Transit datacenter	100 Mbps adresse IP unique	--
Liaisons fibres inter-sites	En cours de remplacement par l'EPMS	Choix porté sur le FAI Linkt

Le candidat devra composer avec l'infrastructure réseau existante. Le lien de transit du datacenter actuel est strictement limité à 100 Mbps et aucune augmentation temporaire de débit ne sera accordée pour les flux de migration. La stratégie de migration des données (messagerie et fichiers) devra être construite pour ne pas impacter le trafic de production des utilisateurs.

La répartition finale (post réorganisation physique) des utilisateurs par site est la suivante :

Site	Adresse	Code postal	Ville	Technologie	Nombre d'utilisateurs
Siege EPMS	Allée André Benoist	77410	CLAYE-SOUILLY	Internet Fibre 200M	104
Ecole PPB(Petits Pas Bleus)	39 Rue Thiers	77124	VILLENNOY	Internet Fibre 100M	34
DSAE Epinette	41 Rue de l'Épinette	77700	MEAUX	Internet Fibre 100M	31
EAM Villenoy	1 Rue Mozart	77124	VILLENNOY	Internet Fibre 100M	19
EAM Mitry	96 Avenue Jean-Baptiste Clément	77290	MITRY-MORY	Internet Fibre 100M	3

2.3.2 Réseau local (LAN) et segmentation

Les sites de l'EPMS disposent de réseaux locaux physiques interconnectés au datacenter par des tunnels VPN IPSec. Les plans d'adressage de ces réseaux locaux ne sont pas documentés à ce stade.



La connectivité inter-sites transite par des pare-feux FORTIGATE infogérés (modèle 60F au siège, modèle 40F sur les autres sites). Le processus de modification des règles de filtrage nécessite une demande externe auprès du prestataire actuel.

Les réseaux locaux de chaque site fonctionnent en architecture plate sans segmentation de sécurité par VLAN. Aucune zone démilitarisée n'existe au niveau des sites, et aucune séparation n'est mise en place entre les utilisateurs administratifs, les équipes médico-sociales et les infrastructures critiques. Tous les utilisateurs et équipements locaux opèrent sur le même segment réseau.

Aucun déploiement Wi-Fi n'a été réalisé sur l'ensemble des cinq sites. Cette absence bloque la mobilité utilisateur intra-site.

Aucune supervision de la couche réseau locale n'est en place.

Les connexions Internet de l'EPMS (liaisons fibres et liens de secours) sont en cours de remplacement par l'établissement et gérées en dehors du périmètre d'infogérance actuel.

2.3.3 Annuaire Active Directory

L'annuaire Active Directory repose sur une infrastructure mono-contrôleur de domaine (serveur en Windows Server 2008 R2, hors support depuis 2020). Depuis la perte de communication du serveur « secondaire », l'ensemble des rôles FSMO (Flexible Single Master Operation) — authentification, rôle de catalogue global, émission des certificats, gestion des permissions - sont concentrés sur ce seul serveur. Cette situation constitue un point de défaillance unique (SPOF) : toute indisponibilité du contrôleur de domaine entraînerait l'arrêt complet de l'authentification pour les agents et l'inaccessibilité de la messagerie Exchange hébergée sur ce même serveur.

Un audit a permis d'identifier 111 ordinateurs connectés au domaine au cours des six derniers mois (plancher minimum observé). L'effectif global de l'établissement est au moment de la rédaction de ce document de 191 utilisateurs.

L'existence d'Unités d'Organisation dédiées à Windows 7 et Windows 8 indique que certaines machines hors support pourraient rester actives sur le réseau. L'établissement procède actuellement au remplacement progressif de ce matériel obsolète.

Les groupes de sécurité ne reflètent pas la structure organisationnelle actuelle (par dispositif, par site, par fonction métier). Les permissions sur les ressources partagées sont souvent attribuées individuellement plutôt que gérées par groupes, compliquant l'audit des droits d'accès. Aucune synchronisation vers un annuaire cloud n'existe actuellement.

Paramètre	État Actuel
Serveur contrôleur domaine	1 seul (Windows 2008 R2, hors support 2020)
Contrôleur secondaire	Défaillant, aucune réplique
Rôles FSMO	Tous concentrés sur le même DC
Ordinateurs domaine inventoriés	111 ordinateurs (6 derniers mois)
Effectif total	191 agents (5 sites)
Groupes de sécurité	Structure peu documentée, peu alignée métier
Synchronisation cloud	Aucune
Politique mot de passe	0 caractère minimum, historique de mot de passe de 24, pas de complexité, pas de MFA

L'EPMS s'engage à fournir au titulaire, dès la réunion de lancement, un fichier consolidé contenant la liste exhaustive des agents actifs, leur direction/service et leur site de rattachement cible.

2.3.4 Messagerie actuelle

La messagerie Exchange 2010 (hébergée sur le contrôleur de domaine) est hors support depuis 2016. La version utilisée est la 14.3 (Build 123.4), Exchange n'a donc pas été mis à jour depuis le SP3. Le serveur gère 253 boîtes aux lettres avec un volume total estimé de 260 Go.

Les archives en fichiers PST (dont le volume total est estimé à 80 gigaoctets) sont fragmentées et distribuées entre serveurs partagés et stockages locaux sur ordinateurs utilisateurs, avec une traçabilité partiellement perdue.

Le certificat en place est autosigné.

La protection des flux sortants s'effectue via un connecteur de transport configuré vers la solution antispam Vade Cloud (smtp.cloud.vadesecure.com). Aucune protection de chiffrement bout-à-bout n'est implémentée de manière native. Les données sensibles de santé transitent en clair par messagerie.

L'absence d'outils de collaboration modernes (Teams, SharePoint) surcharge la messagerie notamment par du partage de fichiers par pièces jointes. Cette pratique fragmente les données, expose les informations sensibles et complique la gestion des droits d'accès.

Paramètre	État Actuel
Nombre de boîtes aux lettres	191 boîtes actives
Volume total stocké	~340 Go (dont 80 Go archives PST fragmentées)
Protocoles supportés	IMAP, POP3, ActiveSync limité, aucun OAuth
Antispam	Vade Cloud (connecteur transport sortant)
Archivage	Aucun processus structuré, PST dispersés
Chiffrement	Zéro (données sensibles en clair)

2.3.5 Serveurs de fichiers et gestion documentaire

L'infrastructure de partage de fichiers repose sur deux serveurs Windows sans gestion de versions et sans récupération granulaire. Les arborescences partagées sont figées et non documentées : aucun inventaire centralisé n'existe, aucun propriétaire n'est formellement attribué, les permissions sont figées depuis des années, une accumulation de dossiers morts et redondants est constatée. Des dossiers redirigés sont utilisés sur plusieurs serveurs.

La volumétrie totale constatée est estimée entre 400 et 500Go dont une grande partie est constituée par les dossiers redirigés des sessions de bureau à distance.

2.3.6 Environnement bureautique et postes de travail

Le parc informatique comprend un mélange hétérogène : 111 ordinateurs intégrés au domaine (PC fixes et portables) plus des clients légers non intégrés à Active Directory. Les clients légers sont de marques HP (en grande majorité), Wise, et potentiellement autres marques. L'établissement ne dispose d'aucun inventaire formalisé centralisé de ce parc. Au démarrage du projet une partie des clients légers aura été remplacée par des clients légers pleinement compatibles avec les charges de travail multimédia en environnement AVD.

La distribution Windows est équilibrée entre Windows 10 et Windows 11. Des unités d'organisation dédiées à Windows 7 et Windows 8 suggèrent la présence possible de machines hors support. L'établissement procède au remplacement progressif de ces équipements.

Aucun système de gestion centralisée (MDM, Intune équivalent) ne supervise ces appareils. La protection antivirus et EDR est assurée par WithSecure EPP & EDR dans le cadre du contrat d'infogérance.

Tous les clients (lourds & légers) utilisent les serveurs RDS pour accéder aux applications métier. La dépendance à une connexion RDS stable est obligatoire, sans flexibilité pour accès local direct aux outils bureautiques.

Type de Poste	Quantité	Configuration/Remarques
Ordinateurs domaine	111	Windows 10/11 équilibrés, certaines UO Windows 7/8 en cours remplacement
Clients légers	~54	HP majorité, Wise, autres marques
Protection antivirus	WithSecure EPP & EDR	Périmètre contractuel : 130 postes
Gestion centralisée	Aucune (MDM/Intune)	À établir

2.3.7 Applications métiers

L'ÉPMS dépend de trois applicatifs critiques externalisés.

- **AIRMES** : application web de gestion des usagers accessible via navigateur. Elle est hébergée chez un éditeur dédié avec certification Hébergeur de Données de Santé.
- **KELIO/BODET** : assure la gestion des temps, pointage et planifications, intégrée à un système de gestion de présences externe. Environ 10 utilisateurs y accèdent directement. Cet applicatif est maintenu jusqu'à une bascule vers solution SaaS prévue en janvier 2027. L'accès se fait au travers d'un navigateur WEB.
- **EMAGNUS** : archive finances et ressources humaines en lecture seule. Accès limité à 2 utilisateurs. Cet applicatif demeure critique pour la conformité légale et doit rester accessible jusqu'en 2027. L'accès à l'applicatif se fait via un raccourci RDP vers le serveur éponyme.
- **ELAP** : L'accès se fait grâce à un raccourci RDP. La cible est un serveur de bureau à distance appartenant à ELAP et donc hors scope du projet de migration.

AIRMES est hébergé en direct par l'éditeur sur une infrastructure HDS. Les deux autres applications sont hébergées chez le prestataire d'hébergement actuel et demeurent accessibles en coexistence par tunnel VPN. Aucun plan de migration ou bascule SaaS n'a été décidé actuellement pour **KELIO/BODET** et **EMAGNUS**.

Application	Hébergement	Utilisateurs	État Actuel
AIRMES	Éditeur externe HDS	~100 accès régulier	Coexistence VPN, tunnel existant
KELIO/BODET	VM Vmware	~10	Maintenu jusqu'à bascule SaaS janvier 2027
EMAGNUS	VM Vmware	2 (RH, Finance)	Lecture seule, archivage, jusqu'en 2027
ELAP	Editeur (externe) ELAP		

2.3.8 Impression

Les imprimantes (une trentaine) de tous les sites sont actuellement toutes configurées sur les serveurs de Bureau à distance. Il n'existe aucune solution de libération de l'impression par badge qui permettrait de sécuriser les impressions de documents confidentiels.

2.3.9 Profils utilisateurs et spécificités d'usage

L'établissement accueille 191 agents répartis sur cinq sites. La population présente une hétérogénéité marquée en matière de familiarité avec l'outil informatique. Une forte part de cette population n'est pas familière avec les technologies informatiques et repose sur des modes opératoires figés et peu autonomes pour résoudre les problèmes techniques.

Les ateliers utilisateurs menés en janvier 2026 ont révélé trois profils d'usage distincts.

- **Le profil administratif** (direction, finances, ressources humaines, secrétariat) concentre des usages intensifs : messagerie, tableur, partages de fichiers, consultation de données archivées. Ces utilisateurs travaillent principalement en poste fixe avec configurations multi-écrans et traitent des dossiers administratifs complexes.
- **Le profil médico-social terrain** regroupe la majorité de la population : éducateurs, infirmiers, travailleurs sociaux. Leurs usages sont légers en termes bureautiques, l'accès au serveur RDS servant principalement à alimenter l'application métier AIRMES. Ces utilisateurs sont distribués sur les cinq sites.
- **Le profil de nomades spécifiques** opère en déploiements extérieurs et travail itinérant. Ces utilisateurs nécessitent des accès distants fiables et une mobilité hors des locaux de l'EPMS, actuellement limités par l'instabilité chronique de l'accès RDS existant et l'insuffisance des forfaits mobiles professionnels.

2.3.10 Contexte d'utilisation et d'accompagnement

L'environnement de travail de l'EPMS et les habitudes des collaborateurs présentent plusieurs spécificités notables :

- **Niveau de maîtrise informatique** : Le niveau d'aisance global avec l'outil informatique est hétérogène et jugé globalement peu élevé. Pour une large partie des collaborateurs (notamment les équipes éducatives et techniques), l'informatique n'est pas l'outil de travail principal.
- **L'établissement opère avec des ressources informatiques limitées** : aucun responsable informatique à temps plein par site. Le support informatique est mutualisé par l'infogérance externalisée avec un délai de réaction standard de 24 à 48 heures. Cette structure crée une dépendance absolue à la stabilité du système : tout incident IT paralyse immédiatement l'opérationnel et génère du stress chez une population peu équipée pour l'auto-dépannage.
- **La culture organisationnelle de l'établissement valorise la fiabilité et la prévisibilité**. Les agents redoutent les changements informatiques non préparés. Les ateliers utilisateurs de janvier 2026 ont révélé des attentes claires : formation présentiel (pas d'e-learning en distanciel seul), support de proximité immédiate en cas de problème, maintien du rôle de l'assistante administrative comme point d'appui utilisateurs.
- **L'informatique parallèle est omniprésente dans les pratiques quotidiennes**. Les groupes WhatsApp personnels servent à la communication d'équipe quotidienne (mélange des sphères privée et professionnelle). Ces contournements reflètent l'absence de solutions institutionnelles performantes et faciles d'accès, non une incompétence ou une insubordination utilisateurs.
- **La direction de l'établissement a exprimé une attente forte** : la migration doit apporter une amélioration opérationnelle visible et immédiate (réduction des lenteurs, accès plus fluide, collaboration facilitée). Sans démonstration rapide de gains concrets, le risque de rejet par la population utilisateurs demeure réel.

2.4 Sécurité actuelle et conformité

2.4.1 Cadre réglementaire et légal

En sa qualité d'Établissement Public Médico-Social, l'EPMS est assujettie à la **Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S)**. Ce cadre réglementaire s'applique à l'ensemble des traitements impliquant des données de santé à caractère personnel au sein de l'établissement.

2.4.2 Mesures de protection des données actuelles

Actuellement, la protection des données et la prévention des fuites d'information reposent principalement sur des actions de sensibilisation menées auprès des collaborateurs.

Il n'existe pas de mesure technique de Prévention de la perte de données (type DLP - Data Loss Prevention), de classification de l'information ou de chiffrement des communications pour prévenir ou contrôler activement la circulation de données sensibles sur les outils bureautiques.

2.4.3 Usages et circulation des données de santé

Bien que les dossiers des usagers soient gérés dans des applications dédiées en mode SaaS, il est constaté que des documents contenant des données de santé (tels que des prescriptions, des ordonnances ou des comptes rendus) peuvent être amenés à circuler et à être échangés via la messagerie électronique actuelle.

Les dossiers d'usagers sont par exemple scannés dans un répertoire avant de pouvoir être intégrés à l'application AIRMES. Ce processus n'est pas documenté, pas contrôlé et le cycle de vie des données pas géré laissant des données personnelles potentiellement accessibles sur des partages communs.

3 Exigences fonctionnelles transverses

Les exigences transverses décrites ci-après constituent le socle fonctionnel commun à l'ensemble de la solution de modernisation. Elles couvrent les besoins métiers et techniques critiques pour les utilisateurs finaux et reposent sur les principes directeurs d'une approche cloud native, d'accompagnement du changement et de continuité opérationnelle.

3.1 Exigences générales (Collaboration, Mobilité, Productivité)

- **Collaboration** : La solution de gestion documentaire permettra aux collaborateurs de travailler de manière plus fluide et intégrée. Les utilisateurs devront pouvoir co-éditer des documents en temps réel, partager des informations de manière sécurisée au sein d'équipes projet ou de services, et centraliser les communications relatives à un sujet ou un projet.
- **Mobilité et accès unifié** : Les utilisateurs devront pouvoir accéder à l'ensemble de leur environnement de travail (messagerie, fichiers, applications) de manière sécurisée, depuis n'importe quel lieu disposant d'une connexion Internet et depuis différents types de terminaux (poste de travail du bureau, ordinateur portable en déplacement).
- **Productivité** : La solution devra offrir une expérience utilisateur accessible et permettant une adoption rapide, notamment pour un personnel peu familier à l'informatique. Le candidat décrit sa stratégie en matière d'ergonomie, formation initiale, support post-migration et mécanismes de feedback utilisateurs pour assurer l'adoption durable de la solution.

3.2 Exigences spécifiques à la messagerie

- Les utilisateurs devront retrouver **l'intégralité** de leurs emails, contacts et calendriers après la migration.
- La solution devra permettre une **gestion simple et intuitive** des boîtes aux lettres partagées, des calendriers d'équipe et des ressources (salles, matériel).
- L'accès à la messagerie devra être possible via un client lourd (Outlook), un client web (navigateur) ainsi que sur smartphone (application mobile), offrant des fonctionnalités équivalentes.

3.3 Exigences spécifiques aux fichiers & à la gestion documentaire

- Les utilisateurs devront pouvoir accéder à leurs fichiers personnels (remplaçant le "Mes Documents" des profils RDS) et aux fichiers partagés de leurs services/projets depuis une interface unifiée.
- La solution devra nativement intégrer une fonctionnalité de **gestion/historique des versions** des documents, permettant de consulter ou de restaurer des versions antérieures d'un fichier.
- Les utilisateurs devront pouvoir partager des fichiers de manière simple et sécurisée avec des collaborateurs internes ou des partenaires externes, en contrôlant les niveaux de permission (lecture seule, modification).

3.4 Exigences spécifiques à la communication & visioconférence

- La solution devra fournir un outil de **messagerie instantanée** pour des échanges rapides, en individuel ou en groupe.
- Les utilisateurs devront pouvoir organiser et participer à des **réunions en visioconférence** de haute qualité, incluant le partage d'écran et l'enregistrement des sessions.
- La plateforme devra permettre la création d'espaces de travail par équipe (canaux) pour centraliser les conversations, les fichiers et les notes relatifs à un même sujet.

3.5 Exigences spécifiques au bureau à distance

- Les utilisateurs devront retrouver un environnement de bureau complet et familier, leur donnant accès à l'ensemble des applications bureautiques et métiers. Le candidat détaille comment il préserve la continuité d'usage : disposition des écrans, disponibilité des applications, processus de lancement inchangés, pas de réapprentissage majeur.
- L'expérience de connexion et d'utilisation devra permettre une productivité fluide pour tâches bureautiques quotidiennes. Le candidat justifie son dimensionnement réseau, architecture AVD, choix d'infrastructure, et s'engage sur les métriques de réactivité (délai ouverture app, latence clavier, etc.).

3.6 Exigences liées aux applications métiers

- L'accès aux applications métiers devra être transparent pour l'utilisateur depuis sa session de bureau à distance, sans changement dans la manière de les lancer.

3.7 Sécurité et conformité

- La solution devra garantir la protection des données sensibles de l'organisation par des mécanismes de chiffrement robustes, tant au repos qu'en transit. Les données devront être stockées de manière à respecter les exigences de résidence et de souveraineté applicables.
- La plateforme devra se conformer aux obligations réglementaires et légales applicables, notamment en matière de protection des données personnelles et d'accès aux données à des fins de contrôle ou d'audit.
- Un dispositif de traçabilité et d'audit permettant de documenter les accès et modifications de données sensibles. Le candidat détaille : événements journalisés (authentification, lecture, modification, suppression, export), couverture par service (Entra ID, Exchange, SharePoint, AVD), rétention logs, alertes configurables, capacité d'investigation/forensic.
- La solution devra fournir des outils simples pour gérer le cycle de vie complet des utilisateurs : création, modification de droits d'accès, suppression et désactivation de comptes, en conformité avec les politiques organisationnelles.
- Un système de gestion des droits d'accès (autorisation) devra permettre une attribution granulaire et flexible des permissions en fonction des rôles et responsabilités de chaque utilisateur, limitant l'accès au strict nécessaire.
- Les utilisateurs devront pouvoir s'authentifier de manière sûre et efficace, avec des mécanismes d'authentification adaptés aux profils d'usage (agents nomades en déplacement, agents travaillant sur sites EPMS). Le candidat devra décrire son approche en matière d'authentification multi-facteurs et d'accès conditionnel, détailler l'expérience utilisateur par profil, et justifier l'équilibre entre le niveau de sécurité et le confort d'usage.
- La solution devra garantir le traitement sécurisé des données de santé à caractère personnel, conformément aux obligations réglementaires applicables à un établissement médico-social.
- Localisation physique : Données de santé stockées exclusivement en Union Européenne (France ou Europe UE), avec contrat Microsoft explicite engagement HDS.
- Le candidat décrit dans son mémoire technique :
 - Certificat HDS (date validité, services couverts)
 - Plan de conformité PGSSI-S (6 piliers appliqués architecture cible)
 - Architecture de séparation données sensibles (si applicable)

- Mesures complémentaires de protection au-delà HDS/PGSSI-S (si proposées)

3.8 Performance et disponibilité

- La solution devra offrir un niveau de disponibilité et de résilience compatible avec les besoins opérationnels, avec des temps de récupération acceptables en cas de panne ou d'incident.
- Les utilisateurs devront bénéficier de temps de réponse prévisibles et acceptables pour leurs tâches quotidiennes. La latence ne devra pas créer de friction perceptible dans l'usage des services collaboratifs, de messagerie ou de fichiers.
- Un plan de continuité et de reprise après sinistre devra garantir que la solution peut supporter des interruptions de service et se rétablir sans perte irréversible de données critiques.
- Le support utilisateur pour incidents et demandes de service fonctionnera 8h00-18h00, du lundi au vendredi (jours ouvrés EPMS), sans astreinte de nuit ou week-end. Les incidents déclarés en dehors de ces horaires seront traités à la reprise du service.

3.9 Gouvernance et opérabilité

- La solution devra être exploitable et supportable, avec une documentation technique complète, des outils de supervision et d'alerte permettant une détection rapide des anomalies et une résolution efficace des incidents.
- Un dispositif de support utilisateur devra être mis en place pour répondre aux questions, résoudre les problèmes et accompagner les utilisateurs dans l'adoption de la nouvelle solution.
- La gestion du cycle de vie de la solution (mises à jour, évolutions, décommissionnement) devra être encadrée par des procédures claires, avec une planification et une communication appropriées pour minimiser les perturbations opérationnelles.

4 Exigences en matière de Responsabilité Sociétale et Environnementale (RSE)

L'EPMS souhaite engager ses partenaires dans une démarche de développement durable active. Le candidat devra démontrer comment il intègre ces enjeux dans l'exécution du marché.

4.1 Volet environnemental ("Numérique responsable")

Le titulaire devra mettre en œuvre des pratiques visant à réduire l'empreinte carbone des services numériques fournis.

- **Optimisation des ressources Cloud (Lot 1 & 2) :**
 - Pour l'environnement Azure, le titulaire devra privilégier des architectures optimisées permettant de limiter la consommation énergétique inutile.
- **Sobriété numérique :**
 - Le titulaire devra favoriser les procédures qui encouragent la sobriété énergétique.
 - Le candidat décrit son engagement en matière de gestion responsable du matériel informatique en fin de vie (scope des équipements concernés, modalités de recyclage/reconditionnement, responsabilités, coûts intégrés ou non au prix, certifications environnementales ISO 14001 ou équivalent).

4.2 Volet social et sociétal

L'EPMS est attachée aux valeurs d'inclusion et d'égalité.

- **Égalité professionnelle :**
 - Le candidat décrira les dispositions concrètes et les engagements qu'il mettra en œuvre spécifiquement dans le cadre de l'exécution de ce marché pour garantir la mixité et l'égalité professionnelle au sein de l'équipe projet dédiée. Il présentera la répartition prévisionnelle (Femmes/Hommes) de cette équipe projet.
- **Insertion et diversité :**
 - Le candidat est invité à présenter ses engagements en faveur de l'insertion professionnelle et notamment de l'emploi de personnes en situation de handicap.

Partie 2 : Spécifications du Lot 1 - Fourniture des licences Microsoft 365, prestation de migration technique & accompagnement des utilisateurs au changement.

5 Description et périmètre du Lot 1

Ce chapitre détaille les objectifs, le périmètre et la nature des prestations attendues pour le Lot 1.

5.1 Objectifs spécifiques du Lot 1

Le titulaire du Lot 1 est responsable de la réussite de l'intégralité du projet de transformation, incluant la fourniture de la solution, sa mise en œuvre technique et l'accompagnement complet des utilisateurs.

Les objectifs majeurs de ce lot sont les suivants :

- **Fournir & construire** : Assurer la fourniture des licences Microsoft 365 adaptées, et déployer une architecture technique complète sur Microsoft 365 et Azure, conformément aux exigences du présent CCTP.
- **Migrer** : Assurer la migration complète, sécurisée et maîtrisée de l'environnement et des données existants (identités, messageries, fichiers PST, données des serveurs de fichiers, profils utilisateurs). Le titulaire propose son plan de bascule (timing, plan de retour arrière) soumis à validation EPMS.
- **Améliorer la productivité et la collaboration** : Offrir aux équipes un environnement collaboratif performant.
- **Sécuriser** : Garantir que la solution cible respecte les exigences de sécurité de l'EPMS, notamment la conformité avec la **PGSSI-S**.
- **Accompagner et former** : Garantir l'adoption de la solution par l'ensemble des collaborateurs. Pour cela, le titulaire devra concevoir et mettre en œuvre un plan complet d'**accompagnement au changement**, de **communication** et de **formation** adapté aux différents profils utilisateurs.
- **Livrer et transférer** : Livrer une plateforme technique stable et performante, ainsi que l'ensemble de la documentation projet (technique et d'accompagnement), et assurer le transfert de compétences nécessaire aux équipes de l'EPMS pour les tâches d'administration courantes.

- **Respecter le délai** : Le projet de migration technique et d'accompagnement devra impérativement être finalisé et prononcé au plus tard le 31 janvier 2027, afin de coïncider avec la rationalisation des sites physiques de l'établissement.

5.2 Périmètre des prestations attendues

La prestation du titulaire du Lot 1 est une prestation globale et forfaitaire qui devra couvrir l'ensemble des composantes suivantes, de leur conception à leur mise en service et jusqu'à l'adoption par les utilisateurs.

5.2.1 Fourniture des licences

Le titulaire devra assurer la fourniture des abonnements Microsoft 365 (Facturé au réel avec justificatif) pour tous les utilisateurs :

- **Exchange Online** : Messagerie et calendrier cloud pour tous les utilisateurs.
- **Teams** : Plateforme de communication unifiée.
- **SharePoint Online** : Gestion de contenu, sites d'équipe.
- **OneDrive Entreprise** : Stockage personnel et synchronisation de fichiers.
- **Microsoft 365 Apps** : Suite bureautique cloud et bureau.
- **Azure Virtual Desktop (AVD)** : Licences d'accès pour bureau virtuel.

5.2.2 Fourniture et configuration de l'infrastructure réseau

Le titulaire devra assurer la fourniture et la configuration de l'infrastructure réseau :

- **Firewalls physiques** : Remplacement des équipements FortiGate sur les 5 sites finaux de l'EPMS.
- **Interconnexion Azure** : Tunnel VPN permanent entre Azure et l'hébergement actuel et tunnels VPN permanents entre les sites clients et Azure.
- **Solution d'impression et badges** : la conception, la fourniture des licences nécessaires, et la configuration de la solution d'impression sécurisée (idéalement avec une solution SAAS).

5.2.3 Prestations de migration technique et d'infrastructure

Le titulaire devra assurer la conception, le déploiement, la configuration et la migration de l'ensemble des services techniques, incluant :

- La migration de l'annuaire Active Directory 'Local' vers **Microsoft Entra ID**.
- La migration de la messagerie (Exchange 2010 et archives PST) vers **Exchange Online**.

- La migration des serveurs de fichiers et des profils RDS vers **SharePoint Online, Teams et OneDrive**.
- La mise en place de **Microsoft Teams** comme solution de communication.
- Le remplacement de l'infrastructure RDS par **Azure Virtual Desktop (AVD)**, incluant la gestion des profils via FSLogix.
- La conception et la mise en œuvre d'un **VPN Site à Site** entre les sites de l'EPMS et le réseau virtuel Azure.
- La conception et la mise en œuvre d'un **VPN Site à Site** entre le réseau virtuel Azure et le prestataire d'hébergement actuel.
- La fourniture du **Dossier d'Exploitation (DEX)** complet et des procédures d'accès (Entrées/Sorties, Mots de passe) dès la clôture du projet, pour assurer l'autonomie immédiate du Client.

5.2.4 Prestations d'accompagnement au changement et de formation

Le titulaire devra assurer la conception et la mise en œuvre de l'ensemble du volet d'accompagnement humain, incluant :

- L'élaboration d'un **plan d'accompagnement au changement et d'un plan de communication** stratégique.
- La création des supports de communication et leur diffusion.
- La conception pédagogique et l'animation des sessions de formation, adaptées aux différents profils utilisateurs et à leurs usages spécifiques (transfert de compétences).
- La mise en place d'un support de **proximité** renforcé lors des phases de bascule.
- La création de supports pérennes (guides de démarrage, fiches pratiques).
- **Le transfert de compétences interne** : Formation du support IT interne de l'EPMS (sur les activités liées aux entrées/sorties des utilisateurs et la gestion des droits et mots de passe).

6 Exigences techniques de la solution cible (Lot 1)

6.1 Exigences d'architecture générale

Le titulaire devra concevoir une architecture technique pour la solution cible qui respecte les principes et exigences transverses suivants :

- **Principe du "Cloud Native"** : Le candidat décrit son architecture cloud (PaaS/SaaS vs IaaS) et justifie ses choix au regard des contraintes EPMS (bande passante, compétences internes, coûts exploitation). Le recours à des machines virtuelles (Infrastructure en tant que Service - IaaS) devra être limité au strict nécessaire et dûment justifié.
- **Performance** : L'architecture devra garantir des performances et un temps de réponse pour l'accès aux données et aux applications au minimum équivalents à ceux de l'environnement existant. Le candidat dimensionne sa solution pour ~110 utilisateurs simultanés AVD. Il décrit ses engagements latence (délai ouverture app, réactivité clavier) et justifie le dimensionnement.
- **Évolutivité** : L'ensemble de l'architecture devra être conçu pour pouvoir s'adapter de manière flexible à une évolution des effectifs de l'EPMS (à la hausse comme à la baisse) sans nécessiter de refonte.
- **Convention de nommage** : Le candidat propose sa convention de nommage (schéma, exemples, documentation) et explique sa cohérence avec standards d'industrie ou bonnes pratiques Microsoft.
- **Documentation technique** : La conception de l'architecture devra être intégralement documentée dans un Document d'Architecture Technique (DAT).

6.2 Exigences pour la fourniture des licences Microsoft 365

Le titulaire devra inclure dans son offre la fourniture des abonnements et licences Microsoft 365 pour l'ensemble des utilisateurs de l'EPMS. Aucun tenant Microsoft 365 au nom de l'EPMS n'existe actuellement.

Le choix des types de licences devra être **justifié et optimisé**. La proposition du candidat devra impérativement prendre en compte :

- **Les besoins fonctionnels** décrits dans le Tronc Commun.
- L'ensemble des **exigences techniques et de sécurité** du présent CCTP, notamment les fonctionnalités de sécurité avancées (protection contre les menaces, Prévention de la perte de données) et les droits d'usage pour Azure Virtual Desktop.

L'offre du candidat devra présenter de manière claire et détaillée :

- Le(s) type(s) de licence(s) proposée(s).

- Le programme de licences Microsoft proposé (en tenant compte du statut de l'établissement).
- Le coût unitaire par utilisateur/par mois et le coût total pour des durées d'engagement de **1 an et 3 ans**.

6.3 Exigences de gestion des identités et des accès (Entra ID)

L'objectif visé à la clôture du projet est un modèle "Full Cloud" où l'ensemble des comptes utilisateurs actifs sera géré et authentifié directement dans Microsoft Entra ID. L'infrastructure Active Directory actuelle a vocation à être intégralement décommissionnée.

Néanmoins, pendant toute la phase de coexistence du projet (notamment pour l'accès aux applications KELIO et EMAGNUS hébergées chez le titulaire sortant), le titulaire devra maintenir les mécanismes de liaison ou de routage nécessaires pour garantir la continuité des accès. Le décommissionnement définitif des serveurs locaux de l'ancien hébergeur en 2027 est exclu du périmètre du Lot 1.

Le titulaire devra concevoir et mettre en œuvre une solution de gestion des identités moderne et sécurisée, basée sur **Microsoft Entra ID comme annuaire cible principal**.

- **Migration de l'annuaire existant** : Le titulaire devra s'appuyer sur l'annuaire Active Directory existant pour mettre en œuvre une méthode de migration des identités (utilisateurs, mots de passe et groupes pertinents) vers Microsoft Entra ID. L'objectif final est que l'EPMS dispose d'une visibilité complète et d'un contrôle total sur la gestion identités Entra ID (provisionnement, droits, audit, déprovisionnement).
- **Authentification unique (SSO)** : La solution devra fournir une expérience d'authentification unique (Single Sign-On) pour l'accès à l'ensemble des applications de l'écosystème Microsoft 365.
- **Authentification forte et accès conditionnel (MFA)**: Pour répondre aux exigences de sécurité (PGSSI-S), le titulaire devra concevoir et mettre en œuvre une stratégie d'authentification forte et d'accès conditionnel pour 100% des comptes utilisateurs devant disposer d'un accès en dehors des sites de l'EPMS.

Cette stratégie devra impérativement résoudre les deux contraintes suivantes :

- Garantir une **authentification multifacteur (MFA) stricte** pour tous les accès en situation de mobilité (hors des locaux de l'EPMS)
- Prendre en compte le fait que **tous les utilisateurs ne pourront pas être équipés d'une solution MFA** (absence de smartphone professionnel pour une partie du personnel, etc.).

Le candidat doit proposer deux scénarios distincts :

- Stratégie MFA pour utilisateurs équipés

- Stratégie alternative de sécurité renforcée (Accès Conditionnel strict) pour utilisateurs sans MFA, acceptée par l'EPMS

Le candidat décrit l'architecture complète et justifie le niveau de protection pour chaque scénario.

- **Gestion des accès dans l'environnement cible** : La gestion des droits d'accès dans la solution cible devra être basée sur des groupes de sécurité gérés dans Microsoft Entra ID, en appliquant le principe de moindre privilège.

L'EPMS de l'Ourcq est actuellement engagée dans une démarche de nettoyage et de rationalisation de son annuaire Active Directory. L'ensemble des comptes dits "génériques" ou "de service partagés" sont en cours de suppression au profit d'identités strictement individuelles et nominatives.

Dès la réunion de lancement du projet, la liste à jour et consolidée des collaborateurs sera fournie au candidat. Le titulaire devra s'appuyer exclusivement sur cette base assainie pour concevoir l'architecture cible dans Microsoft Entra ID et configurer les licences.

6.4 Exigences pour le service de messagerie

Le titulaire devra assurer la migration complète de la plateforme de messagerie existante (Exchange 2010) vers la solution **Exchange Online**, en garantissant la continuité de service et en renforçant significativement le niveau de sécurité.

- **Périmètre de migration complet** : Le titulaire devra assurer la migration de **100% des données** de la messagerie actuelle, ce qui inclut :
 - L'intégralité des boîtes aux lettres (utilisateurs, partagées, salles et équipements) avec tous leurs contenus (emails, calendriers, contacts, tâches).
 - L'intégralité des **archives d'emails stockées dans des fichiers PST**. La découverte, la collecte et l'importation de ces fichiers dans l'environnement cible sont des prestations attendues.
 - Les dossiers publics, dont la migration ou la conversion vers une autre solution (ex: boîte partagée) devra être proposée.
- **Sécurité et conformité** : La configuration de la plateforme Exchange Online devra intégrer un haut niveau de sécurité. Les exigences minimales sont :
 - La mise en œuvre de protections avancées contre l'hameçonnage, les spams et les malwares.
 - La configuration de **politiques de prévention de la perte de données (DLP)** pour identifier, surveiller et protéger la circulation des données de santé à caractère personnel par courriel.
- **Archivage moderne** : Le titulaire devra mettre en œuvre et configurer la fonctionnalité d'**archivage en ligne** d'Exchange Online. Cette solution devra se

substituer à l'archivage actuel basé sur les fichiers PST. Les politiques de rétention et d'archivage automatique devront être définies avec l'EPMS.

- **Gestion et configuration** : La configuration du service devra inclure la gestion des domaines de messagerie, la définition de politiques de quotas pour les boîtes aux lettres et les archives, ainsi que la configuration des accès et des délégations.

6.5 Exigences pour la collaboration et les fichiers (SharePoint / OneDrive / Teams)

Le titulaire devra concevoir et mettre en œuvre une solution de gestion documentaire et de collaboration moderne, en remplacement des serveurs de fichiers actuels et en introduisant de nouveaux outils.

- **Migration des données** : Le titulaire devra assurer la migration de l'ensemble des données des serveurs de fichiers existants vers la plateforme cible, en respectant la répartition suivante :
 - Les **données partagées** devront être migrées vers une architecture **SharePoint Online/Teams** à définir.
 - Les **données individuelles** (incluant les données des profils utilisateurs RDS) devront être migrées vers **OneDrive Entreprise**.
 - Le titulaire devra proposer une stratégie de traitement (archivage ou suppression) pour les **données identifiées comme obsolètes**.
- **Gouvernance et droits d'Accès** : le titulaire devra :
 - Réaliser un **audit et une rationalisation des droits d'accès** existants avant la migration.
 - Proposer et mettre en œuvre un **plan de gouvernance** clair pour SharePoint Online et Microsoft Teams. Ce plan devra à minima définir les règles de création des sites/équipes, les conventions de nommage et la gestion du cycle de vie
- **Fonctionnalités et usages** : le titulaire devra :
 - Configurer et activer la **gestion/l'historique des versions** sur les bibliothèques de documents.
 - S'assurer du bon fonctionnement des fonctionnalités de **coédition** en temps réel.
 - Configurer les **politiques de partage externe** (liens, invités) en accord avec les exigences de sécurité de l'EPMS.
- **Configuration de Microsoft Teams** : le titulaire devra :
 - Assurer la configuration complète de Teams comme hub de communication de l'établissement, incluant les fonctionnalités de **messagerie instantanée, d'appels et de visioconférence**.
 - Proposer une structure d'équipes de départ et configurer l'**accès invité** conformément à la politique de partage externe.

6.6 Exigences pour le bureau à distance (Azure Virtual Desktop)

Justification du modèle architectural AVD : l'EPMS de l'Ourcq a fait le choix stratégique d'une infrastructure Azure Virtual Desktop (AVD) pour répondre à deux contraintes majeures et non négociables de son parc :

- **La pérennisation du parc de terminaux** : L'établissement conserve et maintient l'usage de ses clients légers (environ 54 terminaux de marques HP, Wise, etc.) qui ne disposent pas de la puissance locale pour faire tourner des applications lourdes ou modernes.
- **La standardisation des environnements** : Garantir un environnement de travail unique, performant et fluide, que l'agent se connecte depuis un client léger sur site ou depuis un poste mobile/tablette en situation de nomadisme terrain.

Le titulaire devra concevoir et mettre en œuvre une solution de bureau à distance moderne, performante et flexible basée sur **Azure Virtual Desktop**, en remplacement de l'infrastructure RDS actuelle.

- **Performance et expérience utilisateur** : La solution devra offrir une expérience utilisateur fluide et réactive. La performance devra être garantie y compris lors de pics de charge.
- **Optimisation des Coûts** : Le candidat démontrera comment son architecture adapte les ressources aux variations d'activité quotidiennes/saisonnnières. Il proposera des engagements de coût consommation Azure (ex : coût/utilisateur/mois).
- **Déploiement et mise à jour des applications durant le projet** : Le titulaire devra assurer le **déploiement initial et le maintien à jour** des applications (bureautiques et métiers) sur l'environnement Azure Virtual Desktop, **pour toute la durée du projet de migration**. Il devra décrire dans sa réponse la méthode et les outils qu'il compte utiliser pour garantir une gestion des applications simple, reproductible et sécurisée.
- **Gestion des profils utilisateurs** : La gestion des profils utilisateurs devra être assurée par la technologie **FSLogix** afin de garantir leur persistance et leur itinérance entre les sessions. Le titulaire devra proposer et justifier le choix du service de stockage Azure sous-jacent pour garantir la performance, la résilience et l'optimisation des coûts.
- **Accès sécurisé** : L'accès à l'environnement AVD devra être sécurisé et maîtrisé, en s'appuyant sur les mécanismes de sécurité de Microsoft Entra ID.
- **Visioconférence Teams** : La solution devra permettre aux clients légers de suivre une réunion ou un webinaire Teams (sans pour autant nécessairement utiliser eux-mêmes une webcam).

6.7 Exigences pour la solution de sécurité des terminaux (Antivirus / EDR)

- **Enrôlement et gestion MDM (Microsoft Intune)** : Le titulaire du Lot 1 aura la charge de concevoir l'architecture de gestion des terminaux et d'assurer l'enrôlement complet de l'intégralité du parc de postes lourds et portables de l'établissement, représentant un plancher minimum de **111 ordinateurs** recensés.
- **Sécurité et licences cibles** : La protection des terminaux devra être centralisée et s'appuyer sur la solution Microsoft Defender for Business. Le déploiement de l'agent Defender et l'application des règles de réduction de la surface d'attaque seront entièrement orchestrés via Microsoft Intune.
- **Configuration des politiques** : Le titulaire devra configurer dans Microsoft Intune les profils de configuration des postes, les politiques de conformité et les cycles de déploiement des mises à jour Windows Update pour la sécurité du parc.
- **Périmètre du déploiement** : Le titulaire devra assurer l'enrôlement, la configuration des agents et le déploiement de la solution de sécurité sur l'intégralité du parc de postes lourds et portables de l'établissement, représentant un plancher minimum de 111 ordinateurs recensés.
- **Gestion et configuration via le Cloud (MDM)** : Le déploiement des agents Microsoft Defender, la supervision de leur état de santé ainsi que l'application des politiques de sécurité (mises à jour des signatures, règles de réduction de la surface d'attaque, analyses programmées) devront être orchestrés via la solution de gestion centralisée Microsoft Intune.
- **Orchestration de la transition technique** : L'infrastructure actuelle étant protégée par la solution WithSecure EPP & EDR sous l'égide du contrat d'infogérance sortant, le titulaire du Lot 1 devra obligatoirement décrire dans son mémoire technique sa méthodologie pour assurer une transition transparente. Cette procédure devra garantir la désinstallation propre de l'ancien agent et l'activation immédiate de Microsoft Defender, sans aucune rupture de protection ni de vulnérabilité pour les postes durant la phase de migration.
- **Niveau de protection et conformité** : Les profils de sécurité configurés par le titulaire devront respecter le principe de "sécurité par défaut" et s'aligner sur les exigences de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) applicables à l'EPMS. Cela inclut l'activation des protections en temps réel contre les rançongiciels (ransomwares), les logiciels malveillants et les attaques de type jour zéro.

6.8 Exigences pour le remplacement des pare-feux locaux

Le titulaire devra fournir, configurer, installer et tester les nouveaux équipements de sécurité périmétrique (pare-feux physiques) sur les 5 sites finaux de l'EPMS.

- **Souveraineté et certifications** : Afin de répondre aux exigences strictes de la PGSSI-S et de garantir la souveraineté de la protection des flux de l'établissement, les équipements proposés devront idéalement être avec du matériel souverain disposant d'une qualification standard de l'ANSSI et figurant au catalogue de l'ANSSI pour le secteur public. Si le candidat propose une alternative, il devra obligatoirement prouver qu'elle dispose de certifications européennes ou nationales équivalentes pour le secteur public hospitalier.
- **Dimensionnement et performance** : Les boîtiers matériels devront être dimensionnés pour supporter les débits des liaisons fibres optiques cibles de chaque site, avec l'ensemble des services de sécurité activés (filtrage applicatif, inspection SSL, antivirus de flux) sans dégradation de la latence pour les sessions Azure Virtual Desktop (AVD).
- **Abonnements de sécurité et support** : Le candidat devra inclure dans son offre les abonnements de sécurité comprenant le filtrage d'URL et la prévention des intrusions. Le support constructeur et le remplacement matériel en cas de panne matérielle devront être provisionnés pour une durée minimale cohérente avec le marché.
- **Haute disponibilité des flux (Multi-WAN)** : Les pare-feux devront nativement gérer le basculement automatique (failover) entre les liens fibres principaux et les liaisons de secours de l'EPMS afin de garantir la continuité absolue des tunnels VPN vers Azure.
- **Interconnexion Cloud** : Chaque pare-feu devra être configuré pour monter et maintenir un tunnel VPN permanent, sécurisé (chiffrement AES-256 minimum) et performant vers le réseau virtuel Microsoft Azure conçu dans le cadre du projet.

6.9 Exigences pour les interconnexions (VPN)

Cette section couvre les exigences pour les composants d'infrastructure spécifiques qui devront être déployés sur Microsoft Azure pour supporter l'ensemble de la solution.

- **Mise en œuvre** : Le titulaire devra déployer et configurer une interconnexion de type **VPN Site à Site** entre les sites de l'EPMS et le réseau virtuel Azure. Il devra également déployer et configurer une interconnexion de type VPN Site à Site entre le réseau virtuel Azure et le centre d'hébergement actuel.
- **Performance et fiabilité** : Le tunnel VPN devra être dimensionné pour supporter les flux de communication nécessaires (notamment pour l'impression) de manière fiable et performante.

- **Sécurité** : L'interconnexion devra être configurée en respectant les meilleures pratiques de sécurité.

Le prestataire d'hébergement actuel de l'infrastructure a été formellement informé du présent projet de modernisation.

Le paramétrage, l'ouverture des flux et la configuration du tunnel VPN Site-à-Site du côté de la plateforme vCloud seront exécutés directement par les équipes de l'hébergeur actuel, à la demande de l'EPMS.

Afin de permettre au titulaire du Lot 1 de piloter son planning de déploiement de manière fiable, le prestataire actuel s'est engagé sur un délai maximal de mise en œuvre de [cinq (5)] jours ouvrés à compter de la réception des spécifications techniques de l'interconnexion (fournies par le titulaire du Lot 1). Le titulaire devra intégrer ce délai de prévenance dans son plan de projet détaillé.

6.10 Exigences pour la solution d'impression sécurisée

6.10.1 Choix technologique et architecture générale

Afin de rationaliser ses périphériques d'impression et les sécuriser, l'EPMS a fait le choix de la solution GESPAGE. Le titulaire devra déployer une Machine Virtuelle dédiée hébergée dans l'infrastructure Azure.

L'EPMS contactera GESPAGE directement pour validation fonctionnelle et déploiement de la solution applicative (hors scope Lot 1, mais timing coordonné).

6.10.2 Infrastructure technique – VM d'impression

Le candidat devra :

- Provisionner une VM Windows Server avec les spécifications minimales suivantes :
 - Processeurs : 4 vCPU
 - Mémoire RAM : 8 Go
 - Stockage disque : 100 Go minimum
 - Localisation : région Azure EU
- S'engager à déployer la VM **au plus tôt** dans le projet (idéalement avant fin phase 1 de migration), afin de permettre à GESPAGE d'installer et configurer sa solution dans les délais.
- Assurer la connexion réseau de la VM :
 - Accès HTTPS sortant vers les services Azure (identités, logs)

- Accès réseau interne vers toutes les imprimantes (30 équipements)
- Communication avec AVD et postes de travail pour le driver d'impression.

L'EPMS fournira en amont du démarrage projet la liste exhaustive des ports réseau requis par GESPAGE (entrée/sortie).

6.10.3 Déploiement des imprimantes et configuration GPO

Le candidat devra :

- Créer et déployer les objets de stratégie de groupe (GPO) permettant :
 - L'installation automatique du driver d'impression GESPAGE sur tous les postes de travail (physiques et AVD)
 - La redirection des flux d'impression vers la VM GESPAGE
 - La configuration des paramètres d'authentification (badge/PIN)
- Documenter la stratégie GPO dans le Document d'Architecture Technique (sections : nommage, hiérarchie OU, ordre application, exceptions).
- Valider le déploiement GPO avec l'EPMS avant bascule complète (tests sur vague pilote).
- Assurer la compatibilité du déploiement GPO avec :
 - Azure Virtual Desktop (sessions utilisateurs)
 - Les postes de travail on-site (Windows 10/11)
 - Les profils mobiles et FSLogix

6.10.4 Coordination avec GESPAGE

Le candidat s'engage à coordonner directement avec GESPAGE (ou avec l'EPMS en cas de besoin) pour :

- Confirmer la VM répond aux prérequis d'installation GESPAGE
- Valider le timing de déploiement VM avant bascule utilisateurs

6.11 Exigences transverses de sécurité

La sécurité est un pilier fondamental de la solution cible. Le titulaire devra concevoir et mettre en œuvre une architecture respectant le principe de "sécurité par défaut" et répondant aux exigences réglementaires de l'EPMS.

- **Conformité PGSSI-S** : Le titulaire devra garantir que l'ensemble de l'architecture, des configurations et des processus proposés est en adéquation avec les principes et exigences de la **Politique Générale de Sécurité des**

Systèmes d'Information de Santé (PGSSI-S) applicables à l'EPMS. Il devra le démontrer dans sa réponse.

- **Protection de l'information** : Des mesures techniques devront être mises en place pour protéger les données sensibles, notamment les données de santé. Le titulaire devra :
 - Proposer et mettre en œuvre une stratégie de **classification des données**. Idéalement prévoir à minima 3 catégories :
 - Publique
 - Confidentielle
 - Santé
 - Décrire sa stratégie de protection données sensibles (classification, DLP, alertes). Il justifie les outils choisis face aux données santé de l'EPMS
- **Protection avancée contre les menaces** : La solution devra inclure des mécanismes de protection avancée contre les menaces pour l'ensemble de l'écosystème. Cela inclut, sans s'y limiter, la protection contre l'hameçonnage, les pièces jointes malveillantes, les liens dangereux et les attaques de type Faille jour zéro ("zero-day").
- **Audit et supervision de la sécurité** : Le candidat décrit sa stratégie d'audit et de journalisation (outils, rétention, supervision, alertes) et justifie les choix.
- **Sécurité des accès et des terminaux** : En complément de la stratégie d'authentification forte, le titulaire devra mettre en œuvre des stratégies pour s'assurer que l'accès aux données et services de l'EPMS ne soit autorisé que depuis des terminaux répondant à un niveau de conformité et de sécurité minimal.
- **Garanties relatives au traitement des données de santé (Prestation de migration)** : Le titulaire, en sa qualité de sous-traitant amené à opérer sur un environnement contenant des données de santé à caractère personnel, devra **décrire dans son offre les mesures techniques et organisationnelles** qu'il met en place pour garantir la sécurité, la confidentialité et la traçabilité de ses interventions durant l'intégralité de sa prestation (habilitation de son personnel, non-consultation des données, chiffrement des flux de migration, etc.).
- **Hébergement des données** : Toutes les données sont hébergées exclusivement en région Azure EU. Aucun transfert de données hors EU n'est autorisé. Le candidat devra attester de la localisation de l'hébergement et de cette conformité dans son offre.
- **Certification** : Le candidat justifie son niveau de maturité en sécurité (certifications, audits externes, référentiel reconnu).

6.12 Exigences d'administration et d'exploitation

À l'issue du projet, les équipes de l'EPMS devront disposer des accès et des outils nécessaires pour administrer la plateforme au quotidien de manière autonome.

- **Accès à l'administration déléguée** : Le titulaire devra configurer des rôles d'administration déléguée pour les équipes de l'EPMS (notamment le responsable informatique actuel), en appliquant le principe de moindre privilège. Les équipes désignées devront pouvoir réaliser les tâches courantes (ex : gestion des utilisateurs, des groupes, réinitialisation de mots de passe) sans disposer de droits d'administrateur global.
- **Supervision et rapports** : Le titulaire devra s'assurer que les équipes de l'EPMS ont accès et sont formées aux tableaux de bord et rapports standards de Microsoft 365 et Azure. L'accès devra inclure à minima :
 - La supervision de l'état des services.
 - Le suivi des rapports d'activité des utilisateurs.
 - Le suivi des coûts de consommation Azure.
 - La consultation des alertes de sécurité de base.
- **Gestion du cycle de vie des utilisateurs et des licences** : Les processus d'arrivée, de modification de rôle et de départ d'un collaborateur devront être simples et documentés. Le titulaire devra fournir la procédure pour l'assignation et la libération des licences Microsoft 365.

7 Exigences d'accompagnement au changement et formation

Le titulaire du Lot 1 est responsable de la réussite de l'adoption de la solution par l'ensemble des utilisateurs. La prestation d'accompagnement est considérée comme un "transfert de compétences" et un accompagnement sur mesure, plutôt qu'une formation générique.

Le titulaire devra concevoir et mettre en œuvre une démarche complète d'accompagnement qui couvrira à minima les exigences suivantes.

7.1 Stratégie et planification

- **Cadrage de l'accompagnement** : Le titulaire devra baser sa stratégie sur le contexte humain de l'EPMS (décrit en section 2.2.9), notamment le niveau de maîtrise informatique hétérogène, les usages peu fréquents pour certains, et les populations identifiées comme plus en difficulté.
- **Plan d'accompagnement au changement** : Le titulaire devra produire un Plan d'Accompagnement détaillé, présentant sa méthodologie, le calendrier des actions, les messages clés et les supports.
- **Synchronisation** : Le planning des actions d'accompagnement (communication, formation) devra être **parfaitement synchronisé** avec le planning de déploiement technique.

7.2 Communication

- **Plan de communication** : Le titulaire devra concevoir et mettre en œuvre un plan de communication adapté aux différentes populations.
- **Canaux prioritaires** : Compte tenu des habitudes de l'EPMS, la communication devra **prioriser les réunions d'équipe en présentiel** (à organiser via la Direction et les responsables de service) plutôt que les communications par email.
- **Supports** : Le titulaire devra produire l'ensemble des supports nécessaires.

7.3 Ingénierie pédagogique et formation

- **Adaptation aux profils** : Le titulaire devra concevoir des modules (les supports seront fournis à l'EPMS dans un format éditable) de formation concrets et distincts pour les deux profils :
 - **Profil "Standard"** : La formation devra être focalisée sur la **transition des usages** ("Avant/Après") et la **collaboration de base sur les fichiers**. L'usage de Teams sera minimal.
 - **Profil "Administratif/Cadre"** : La formation devra couvrir des usages plus avancés (publication SharePoint, organisation de réunions Teams, etc.).
- **Contenu transverse** : Tous les modules de formation devront intégrer un volet de **sensibilisation à la sécurité**, adapté au public.
- **Format et organisation** : La formation devra respecter les contraintes organisationnelles de l'EPMS :
 - Les sessions devront être organisées par **groupes (20-30 personnes maximum)**.
 - Le format privilégié est la **journée complète**, par équipes entières, lors des journées sans accueil du public.
 - **Pédagogie** : une **forte capacité de vulgarisation** et d'adaptation pédagogique à un public peu averti est requise.

7.4 Support post-migration

- **Relais Internes** : Le titulaire devra s'appuyer sur le réseau de **référénts "AIRMES"** existants. Il devra leur fournir une formation spécifique pour leur permettre d'agir comme relais de support de proximité.
- **Support Renforcé** : Le titulaire devra assurer un support renforcé lors de la bascule de chaque vague d'utilisateurs. Le candidat définit son modèle de support (horaires, canaux, SLA réponse) et s'engage sur des délais de traitement.

8 Méthodologie et livrables Attendus pour le Lot 1

8.1 Gouvernance et gestion de projet

Le candidat devra décrire dans son offre la méthodologie de gestion de projet qu'il compte appliquer pour l'ensemble des prestations du Lot 1 (techniques et accompagnement).

- **Chef de projet dédié** : Le candidat devra désigner un chef de projet unique, expérimenté et francophone, qui sera l'interlocuteur principal de l'EPMS et de son AMOA pour toute la durée du projet.
- **Instances de pilotage** : Le candidat devra proposer une structure de gouvernance incluant à minima un **Comité de Pilotage (COPIL)** pour le suivi stratégique et un **Comité de Projet (COPROJ)** pour le suivi opérationnel. Il devra proposer dans son offre une fréquence pour ces instances, qui sera validée lors de la réunion de lancement du projet.
- **Suivi et rapports** : Le candidat structure ses rapports (avancement %, risques/problèmes, capacités consommées) et propose un format adéquat.

8.2 Livrables attendus

Le titulaire devra produire et soumettre à la validation de l'EPMS l'ensemble des documents listés ci-dessous, en français et au format électronique. Cette liste fusionne les attendus techniques et ceux liés à l'accompagnement.

Livrables de pilotage (transverses) :

- Plan d'Assurance Qualité (PAQ)
- Plan de Projet Détaillé
- Rapports d'avancement hebdomadaires (COPROJ)
- Supports de Comité de Pilotage (COPIL)
- Registre des risques

Livrables techniques (liés à la migration) :

- Compte rendu de l'audit de pré-migration
- Document d'Architecture Technique (DAT)
- Stratégie de migration des données
- Plan de tests et Cahiers de Recette (VABF / VSR)
- Dossier d'Exploitation (DEX)
- Procès-Verbaux (PV) de recette (pilote, vagues, globale)
- Bilan de projet (volet technique)

Livrables d'accompagnement au Changement :

- Plan d'Accompagnement au Changement
- Plan de Communication
- Ensemble des supports de communication produits
- Ensemble des supports de formation (par module/profil, format éditible)
- Guides de démarrage rapide / Fiches pratiques
- Bilan de fin de mission (volet accompagnement)

8.3 Exigences de tests et recette

La recette a pour objectif de vérifier la conformité de la solution livrée et des prestations réalisées (techniques et d'accompagnement) par rapport aux exigences du présent CCTP. Chaque phase majeure du projet fera l'objet d'une recette formalisée par un Procès-Verbal (PV).

- **Cahier de recette** : Pour chaque phase de recette, le titulaire devra rédiger un **Cahier de recette** détaillé et le soumettre à la validation de l'EPMS. Ce document devra inclure à minima :
 - La liste des fonctionnalités et exigences techniques à tester.
 - Les scénarios de tests détaillés (prérequis, étapes, données de test).
 - Les résultats attendus pour chaque scénario.
- **Phases de recette** : Le processus se déroulera en deux temps :
 - **La vérification d'aptitude au bon fonctionnement (VABF)** : Il s'agit de la phase de tests internes menée par le titulaire. À l'issue de cette phase, le titulaire devra fournir le cahier de recette dûment complété, attestant que la solution est prête à être testée par l'EPMS.
 - **La vérification de service régulier (VSR)** : Il s'agit de la phase de recette menée par l'EPMS, assistée de son AMOA. La VSR consiste à exécuter tout ou partie des scénarios du cahier de recette pour valider le bon fonctionnement de la solution en conditions réelles.
- **Gestion des anomalies** : Toute non-conformité ou dysfonctionnement constaté lors des phases de recette sera qualifié d'anomalie et consigné dans un registre. Les anomalies seront classifiées selon leur criticité (Bloquante, Majeure, Mineure). L'approbation formelle de la recette définitive ne pourra avoir lieu qu'après correction par le titulaire de l'ensemble des anomalies bloquantes et majeures.

8.4 Transfert de compétences

L'un des objectifs du projet est de garantir l'autonomie des équipes de l'EPMS (notamment le responsable informatique) sur les tâches d'administration et d'exploitation courantes de la nouvelle plateforme, en préparation du futur Lot 2 (Infogérance)

- **Plan de formation** : Le titulaire devra élaborer et dispenser un programme de formation à destination du personnel technique et administratif désigné par l'EPMS.
- **Contenu de la formation** : La formation devra couvrir à minima les sujets définis dans la section **6.9 (Exigences d'Administration et d'Exploitation)**, notamment la gestion des utilisateurs, des licences, et la lecture des tableaux de bord.
- **Support documentaire** : Cette formation devra s'appuyer sur le **Dossier d'Exploitation (DEX)**, qui servira de support de référence pour les équipes de l'EPMS.
- **Accompagnement** : Des sessions de formation de type "compagnonnage" sont attendues, où le titulaire accompagnera les équipes de l'EPMS dans la réalisation de leurs premières tâches d'administration.

Partie 3, dédiée au Lot 2 : Infogérance

9 Description et périmètre du Lot 2

Ce chapitre détaille les objectifs et le périmètre des prestations d'infogérance et de Maintien en Condition Opérationnelle (MCO) attendues pour le Lot 2.

9.1 Objectifs spécifiques du Lot 2

Le titulaire du Lot 2 sera le partenaire de confiance de l'EPMS pour garantir le bon fonctionnement, la sécurité, et l'évolution de son système d'information.

Les objectifs majeurs de ce lot sont les suivants :

- **Garantir la continuité** : Assurer la disponibilité et la performance de l'environnement Microsoft 365 et Azure (Tranche Ferme) et, le cas échéant, de l'infrastructure locale (Tranche Optionnelle).
- **Assurer le support** : Fournir une assistance technique réactive et efficace aux utilisateurs de l'EPMS.
- **Sécuriser & optimiser** : Superviser activement la sécurité de la plateforme, gérer les coûts de consommation Azure et proposer des optimisations continues.
- **Concevoir, mettre en œuvre et exploiter la sauvegarde** : Le titulaire devra concevoir, fournir, mettre en œuvre et assurer l'exploitation complète de la solution de sauvegarde pour l'ensemble de l'environnement cloud (Microsoft 365 et Azure IaaS).

9.2 Périmètre des prestations attendues

Le marché est décomposé en une tranche ferme et une tranche optionnelle.

9.2.1 Tranche Ferme (Obligatoire) : Infogérance de l'écosystème Cloud

Le périmètre de la tranche ferme couvre l'intégralité de l'environnement MS365 et Azure mis en place par le Lot 1. Les prestations incluent :

- **Administration et exploitation des services M365** :
 - La gestion quotidienne des identités (Microsoft Entra ID), de la messagerie (Exchange Online), de la collaboration (SharePoint/Teams) et des politiques de sécurité associées.

- **Support aux utilisateurs :**

- La fourniture d'un guichet unique pour l'ensemble des utilisateurs de l'EPMS, sur la plage horaire 8h-18h (hors astreinte).

- **Administration et exploitation des services Azure :**

- La supervision et l'optimisation des coûts d'Azure Virtual Desktop (AVD).
- Le support et l'administration de la solution d'impression SaaS configurée au Lot 1.
- Le maintien en condition opérationnelle des VPN Site-to-Site.
- Le Maintien en Condition Opérationnelle (MCO) de l'ensemble des services Azure déployés au Lot 1, incluant la machine virtuelle applicative GESPAGE, en termes de disponibilité, performance et sécurité.

- **Supervision et sécurité :**

- La supervision proactive de la sécurité, la gestion des alertes et les rapports associés (semestriel ou sur incident).
- L'infogérance des Pare-feux locaux (au nombre de 5).

- **Mise en œuvre et exploitation de la sauvegarde :**

- La conception, la fourniture, et la mise en œuvre de la solution de sauvegarde pour Microsoft 365 et la VM Azure, en respectant une durée de rétention de 10 ans.
 - Microsoft 365 couvre : Intégralité des boîtes Exchange Online, SharePoint Online, OneDrive Entreprise, Microsoft Teams.
 - VM Azure : VM applicative GESPAGE + ses stockages associés (OS disks + data disks)
 - Restauration granulaire : à l'élément (courriel, fichiers)
- L'exploitation quotidienne de cette solution (supervision, tests de restauration semestriels, exécution des demandes de restauration).

9.2.2 Tranche Optionnelle (Facultative) : Infogérance du parc local

Le candidat devra chiffrer dans une option séparée la reprise en infogérance de l'infrastructure et du parc local de l'EPMS.

Le périmètre de cette tranche optionnelle inclut à minima :

- **Gestion et support des postes clients :**

- Le support matériel et logiciel (diagnostic, garanties) du parc de postes.
- L'achat, le paramétrage et la mise en service des nouveaux postes.

- L'enrôlement et la gestion centralisée (via Entra ID/Intune) de l'ensemble du parc de postes lourds.
- **Gestion du réseau local (LAN/Wifi) :**
 - Le Maintien en Condition Opérationnelle des équipements réseau.
- **Gestion de la connectivité :**
 - La supervision du lien Internet. Le contact avec le FAI (Linkt) reste à la charge de l'EPMS, le titulaire assurant le pilotage technique.
- **Gestion des périphériques :**
 - Le support et la gestion des incidents liés aux périphériques d'impression (y compris les imprimantes de bureau non gérées par la solution centrale).
- **Support de proximité :**
 - Une présence sur site **d'une journée par semaine** (modulable selon les besoins).
 - La capacité à fournir des interventions sur site complémentaires (sur commande) pour la résolution des incidents matériels bloquants.
- **Services exclus :**
 - La gestion de la **Téléphonie IP** est explicitement **exclue** du périmètre de cette tranche optionnelle.

9.3 Livrables et interface Lot 1 → Lot 2

Le Lot 1 remet intégralement au Titulaire du Lot 2, à titre de **documentation de base** pour l'exploitation :

- **DEX (Document d'Architecture Existante) :** Architecture Microsoft 365 et Azure déployée
- **Documents d'Architecture détaillée :** Configurations exportées (stratégies, groupes, paramètres du tenant)
- **Liste des services Azure :** Inventaire des VM, AVD pools, storage, VPN, Azure ressources
- **Accès documentés :** Mots de passe/secrets remis via gestionnaire sécurisé
- **Tests de validation :** Rapports VSR (Vérification Service Rendu) et VABF (Acceptation avant Facturation)



Le titulaire du Lot 2 participera aux réunions de transfert technologique de fin de projet du Lot 1. Dès la remise des livrables du Lot 1 (DEX, configurations), le titulaire du Lot 2 disposera d'un délai de carence de quinze (15) jours calendaires pour analyser l'environnement et émettre d'éventuelles réserves techniques. Passé ce délai et après résolution des points bloquants, le titulaire signera le Procès-Verbal de Reprise de la Plateforme, matérialisant le transfert de responsabilité du MCO.

10 Exigences pour les prestations d'infogérance (Lot 2)

10.1 Exigences d'administration et d'exploitation des services M365

Le titulaire sera responsable du bon fonctionnement, de la sécurité et de l'évolution des services Microsoft 365. Ses missions incluront à minima :

- **Gestion des identités (Entra ID) :**
 - Gestion du cycle de vie des utilisateurs (arrivées, départs, modifications) en coordination avec les RH de l'EPMS.
 - Gestion des groupes de sécurité et de distribution.
 - Administration et ajustement des politiques d'Accès Conditionnel et d'Authentification Multi Facteur, en accord avec l'EPMS.
 - **Gestion déléguée des invitations** pour les contacts externes (invités).
 - **Gestion déléguée de la réinitialisation des mots de passe.**
- **Gestion de la messagerie (Exchange Online) :**
 - Gestion des boîtes aux lettres (création, modification, conversion en boîte partagée, etc.).
 - Gestion des listes de distribution.
 - Traitement des incidents de messagerie (ex : problèmes de flux, spams non bloqués).
- **Gestion de la collaboration (SharePoint / Teams) :**
 - Administration de la gouvernance des sites SharePoint et des Équipes Teams (application des règles de création, de nommage, d'archivage).
 - Gestion des droits d'accès complexes et des politiques de partage externe, sur demande validée.

10.2 Exigences de support aux utilisateurs (Centre de services)

Le titulaire devra fournir un service de support (guichet unique ou "Centre de Services") réactif et efficace pour l'ensemble des utilisateurs de l'EPMS, couvrant l'intégralité du périmètre de la Tranche Ferme (et de la Tranche Optionnelle, si levée).

- **Canaux de contact :** Le titulaire devra fournir plusieurs moyens de contact, en **priviliégiant le canal téléphonique** (numéro d'appel unique), qui est l'usage

principal de l'EPMS. Un portail web et une adresse email de support devront également être fournis.

- **Horaires de service** : Le support devra être disponible et joignable durant les jours et heures ouvrés de l'EPMS, soit de **8h00 à 18h00, du lundi au vendredi**, hors jours fériés. Il n'est **pas attendu de service d'astreinte** en dehors de ces horaires.
- **Gestion des demandes (Incidents et Services)** :
 - Le titulaire utilise un outil de gestion des tickets certifié ITIL/ITSM et garantit l'enregistrement de 100% des sollicitations.
 - Le Titulaire décrira son modèle opérationnel du Centre de Services, incluant notamment :
 - Nombre d'agents, taille équipes/escalade
 - Horaires de couverture 8h-18h (hors astreinte) : comment assurer continuité et pics ?
 - Processus d'escalade vers éditeur Microsoft/Azure
 - Indicateurs KPI qualité
 - Intégration ITSM : outils utilisés (ServiceNow, Jira SM, etc.) ou justifier choix.
- **Périmètre du support** : Le support couvrira à minima :
 - L'assistance à l'utilisation des services Microsoft 365 (Outlook, Teams, OneDrive, SharePoint...).
 - La résolution des incidents liés à l'accès et à la performance d'Azure Virtual Desktop (AVD).
 - La gestion des problèmes de connectivité liés à l'écosystème cloud (VPN).
 - La réinitialisation de mots de passe.
 - L'assistance bureautique de base.
- **Amélioration continue** :
 - Le titulaire devra maintenir une base de connaissances des résolutions.
 - Le titulaire identifie proactivement les problèmes récurrents et propose des actions correctives pérennes.

10.3 Exigences d'administration et d'exploitation des services Azure

Le titulaire du Lot 2 sera responsable du Maintien en Condition Opérationnelle (MCO) et de l'administration active de l'ensemble des services et ressources déployés sur la plateforme Microsoft Azure.

- **Gestion d'Azure Virtual Desktop (AVD) :**
 - Le candidat décrira sa stratégie et ses outils pour assurer la maintenance continue de l'image golden AVD. Détaillez notamment : (a) fréquence des mises à jour OS/applicatif, (b) processus de test avant déploiement, (c) plan de rollback en cas d'anomalie, (d) capacité à restaurer une version antérieure en < 1h en cas de problème.
 - Le candidat proposera et justifiera son approche d'élasticité AVD. Il détaillera notamment : les critères de déclenchement, les configurations testées en termes de pic et creux de nuit, les engagements de coût mensuel prévisible avec variance admise, la capacité à basculer en mode manuel en cas de perturbation.
 - Il devra gérer la capacité et la performance du stockage des profils FSLogix.
- **Gestion de l'interconnexion réseau (VPN) :**
 - En cas de coupure du tunnel VPN (identifié comme un service critique), le titulaire sera le point d'entrée unique pour le diagnostic et le pilotage de la résolution, en coordination avec les éventuels autres partis (fournisseur d'accès Internet, etc.).

10.4 Exigences de supervision et de sécurité

Le titulaire du Lot 2 sera responsable de la surveillance active de l'ensemble de la plateforme cloud (Tranche Ferme) pour en garantir la performance, la disponibilité, la maîtrise des coûts et la sécurité.

- **Supervision de la performance et de la disponibilité :**
 - Le titulaire devra mettre en œuvre une supervision proactive de l'état de santé et de la performance de l'ensemble des services de la Tranche Ferme (Microsoft 365, AVD, VM, VPN).
 - Il devra intervenir pour résoudre les dégradations de service avant qu'elles n'impactent significativement les utilisateurs.
- **Supervision et optimisation des coûts :**
 - Le titulaire devra superviser activement la consommation des ressources Azure et alerter l'EPMS en cas de dérive anormale par rapport aux prévisions.
 - Il devra fournir des analyses et des **recommandations d'optimisation proactives** (à inclure dans le rapport mensuel).
- **Sécurité opérationnelle :**
 - Le titulaire devra assurer **la supervision continue des alertes de sécurité** issues des portails Microsoft.

- Il sera responsable du **Maintien en Condition Opérationnelle (MCO) des politiques de sécurité** (Prévention de la Perte des Données, Accès Conditionnel) configurées par le Lot 1.
- Il devra gérer la **remédiation des incidents de sécurité de premier niveau** (ex : blocage d'un compte compromis, analyse d'un email d'hameçonnage).
- Le Candidat proposera dans son offre un processus clair de gestion et d'escalade pour les incidents de sécurité. Le Titulaire s'engage contractuellement sur l'exécution de ce processus

10.5 Exigences de mise en œuvre et d'exploitation de la sauvegarde

La conception, la fourniture, la mise en œuvre et l'exploitation de la solution de sauvegarde relèvent intégralement du périmètre de ce Lot 2 (Tranche Ferme).

10.5.1 Conception et mise en œuvre

- Le titulaire devra **proposer, fournir (licences/service)** et mettre en œuvre une solution de sauvegarde complète et externalisée.
- Le périmètre de sauvegarde devra couvrir à minima :
 - **Microsoft 365** : L'intégralité des données des services Exchange Online, SharePoint Online, OneDrive Entreprise et Microsoft Teams.
 - **VM Azure**

10.5.2 Exigences fonctionnelles et de rétention

- La solution devra impérativement permettre la **restauration granulaire** (à l'élément : email, fichier, etc.).
- La solution devra garantir une **conservation (rétention) des données sur une durée de 10 ans**.
- Conformément à la PGSSI-S, les données devront impérativement être localisées en Europe et idéalement chez un hébergeur HDS.

10.5.3 Exigences d'exploitation quotidienne

- Le titulaire assurera la **supervision journalière** de la bonne exécution des sauvegardes.
- Il sera responsable de la **gestion des alertes** et de la **remédiation** en cas d'échec.
- Il assurera l'exécution des **demandes de restauration** (granulaire ou complète) de l'EPMS.
- Il devra réaliser des **tests de restauration périodiques** (a minima **semestriels**) et fournir les comptes rendus de ces tests à l'EPMS.

10.6 Exigences d'administration et d'infogérance des firewall

Le titulaire du Lot 2 sera responsable de l'infogérance complète des équipements firewall mis en place par le Lot 1, garantissant la disponibilité, la sécurité et les performances de la sécurité périmétrique de l'EPMS.

10.6.1 Supervision et métrologie

Le titulaire devra mettre en œuvre une supervision proactive des 5 équipements firewall déployés sur les sites de l'EPMS.

- **Outillage de supervision :**
 - Le titulaire déploiera un outil de monitoring et d'alerte permettant la surveillance en temps réel de l'état opérationnel des firewalls (CPU, mémoire, connectivité, sessions actives).
 - Les seuils d'alerte devront être configurés et validés avec l'EPMS pour les indicateurs critiques (charge CPU >80%, mémoire >85%, perte de connectivité).
 - Le candidat s'engage à fournir un tableau de bord accessible à l'EPMS permettant la visualisation en temps réel du statut des équipements.
- **Rapports de performance :**
 - Le titulaire intégrera dans son rapport mensuel une analyse de la performance des firewalls (taux d'utilisation, incidents de blocage, anomalies détectées).
 - Identification proactive des tendances anormales et recommandations correctives.

10.6.2 Maintien en Condition Opérationnelle (MCO)

Le titulaire sera responsable du maintien en conditions de sécurité et de performance des équipements firewall.

- **Gestion des mises à Jour :**
 - Le candidat décrira dans son offre son processus de gestion des mises à jour firmware, notamment :
 - Fréquence des mises à jour de sécurité (a minima mensuellement ou à titre critique selon avis du fabricant)
 - Planification des interventions en coordination avec l'EPMS (fenêtres de maintenance acceptables)
 - Plan de rollback en cas d'anomalie post-mise-à-jour

- Le candidat s'engage à rétablir l'équipement en version antérieure en moins d'1 heure en cas de dysfonctionnement suite à une mise à jour.

- **Gestion des configurations :**

- Le titulaire assurera le versioning et la documentation des configurations firewall (règles, politiques, listes noires/blanches).
- Toute modification de configuration devra être tracée, documentée et justifiée.
- Une sauvegarde centralisée et sécurisée des configurations sera maintenue et testée régulièrement.

- **Maintenance préventive :**

- Inspections régulières du bon fonctionnement des équipements (tests de basculement redondance si applicable).
- Tests mensuels de continuité en cas de perte d'un firewall (si architecture redondante).
- Optimisation des règles de filtrage pour éviter les surcharges.

10.6.3 Gestion des incidents de sécurité réseau :

Le titulaire sera le point d'entrée unique pour la gestion opérationnelle des incidents affectant la sécurité périmétrique.

- **Incidents de sécurité :**

- Monitoring continu des alertes de sécurité remontées par les firewalls (tentatives d'intrusion, attaques détectées, trafic suspect).
- Escalade immédiate vers l'EPMS et la direction en cas de menace grave ou tentative d'intrusion confirmée.
- Analyse de premier niveau et blocage/déblocage d'adresses IP ou trafic selon directives de l'EPMS.
- Documentation des incidents (historique complet pour traçabilité).

- **Gestion des listes Noires/Blanches :**

- Traitement des demandes de blocage/déblocage d'adresses IP, domaines ou ports.
- Justification technique des règles mises en place.

10.6.4 Engagements de service (SLA)

Le candidat devra proposer lui-même dans son offre des engagements clairs sur les niveaux de service relatifs aux firewalls, en s'appuyant sur les définitions de priorité définies en section 10.7.1 du présent CCTP.

Sa proposition devra détailler :

- **Temps de prise en charge :**
 - P1 (Perte de connectivité firewall / attaque active)
 - P2 (Dégradation de performance / alerte mineure)
 - P3 (Demande de modification non urgente)
- **Temps de rétablissement :**
 - P1 : Rétablissement en moins de X heures
 - P2 : Rétablissement en moins de X heures
 - P3 : Rétablissement selon planification à convenir

10.6.5 Intégration aux processus de gouvernance

- Les incidents et changements affectant les firewalls seront documentés dans les rapports mensuels et discutés lors du Comité de Pilotage mensuel.
- La gestion des incidents de sécurité réseau sera intégrée au processus global de gestion des crises de sécurité défini en section 10.4.

10.7 Exigences de pilotage, qualité de service et comitologie

Le titulaire devra s'engager sur un ensemble d'indicateurs et de processus garantissant la qualité et la transparence de la prestation d'infogérance (Tranche Ferme).

10.7.1 Définition des niveaux de priorité

Le titulaire devra s'appuyer sur la classification de priorité suivante pour formuler ses engagements de service :

- **Priorité 1 (P1 - Bloquant) :** Incident rendant indisponible un service critique pour l'ensemble de l'EPMS ou pour un service entier (ex : panne AVD, coupure VPN, DLU inaccessible).
- **Priorité 2 (P2 - Majeur) :** Incident dégradant fortement l'utilisation d'un service critique ou le rendant indisponible pour un utilisateur ou un groupe.
- **Priorité 3 (P3 - Mineur) :** Incident n'impactant pas la production ou demande de service courante.

10.7.2 Engagements de niveaux de service

Le titulaire devra proposer lui-même et s'engager contractuellement sur des Niveaux de Service (SLA) clairs, en s'appuyant sur les définitions de priorité fixées en 10.6.1.

Sa proposition devra détailler :

- Ses **temps de prise en charge** pour chaque niveau de priorité.

- Ses **temps de rétablissement** pour chaque niveau de priorité.

10.7.3 Gouvernance et suivi de service

- **Instances de suivi :**
 - Le titulaire devra animer un **Comité de Pilotage (COPIL)** à une fréquence mensuelle.
- **Objectif du comité :**
 - Revoir le rapport d'activité du mois écoulé.
 - Analyser les incidents marquants et les problèmes récurrents.
 - Suivre le respect des engagements de niveaux de service.
 - Discuter des optimisations (notamment les coûts Azure).
 - Passer en revue les incidents de sécurité. Et l'état de la plateforme.

10.7.4 Rapports d'activité

Le titulaire devra fournir un **rapport d'activité mensuel** avant chaque comité de suivi. La fréquence de ce rapport pourra évoluer au cours du marché, après accord entre les parties.

Ce rapport devra inclure à minima les indicateurs de performance clés suivants :

- **Gestion des coûts :**
 - Le suivi détaillé des coûts de consommation Azure, avec une analyse des variations par rapport aux prévisions et des préconisations d'optimisation.
- **Activité du support :**
 - Le volume de tickets (ouverts, fermés, en cours) par priorité et par service.
 - Une **analyse des typologies de tickets** afin d'identifier les problèmes récurrents, les axes d'amélioration ou les besoins de sensibilisation des utilisateurs.
- **Performance du service :**
 - Le **taux de respect des engagements de niveaux de service** proposés par le titulaire dans son offre.
- **Activité de sauvegarde :**
 - Un **suivi de l'état des sauvegardes** et le compte rendu des tests de restauration semestriels.
- **Activité sécurité :**
 - Un **rapport de sécurité semestriel** résumant l'état de la plateforme, (sauf incident majeur nécessitant un rapport immédiat).

10.8 Exigences relatives à la tranche optionnelle (parc local)

Le candidat devra chiffrer dans une **Tranche Optionnelle (TO)** séparée la prise en charge de l'infogérance de l'infrastructure et du parc local, **dont le périmètre est défini en section 9.2.2.**

Si l'EPMS décide de lever cette option au cours du marché, le titulaire s'engage à réaliser ces prestations en les intégrant dans le cadre de service global défini pour la Tranche Ferme.

Les exigences suivantes s'appliqueront :

- **Gouvernance et rapports :**
 - Les prestations de la Tranche Optionnelle devront être intégrées dans les instances (Comité de Pilotage) et les rapports mensuels (indicateurs spécifiques à définir) prévus à la section 10.6.
- **Support aux utilisateurs :**
 - Le Centre de Services (défini en 10.2) devra devenir le guichet unique également pour les incidents liés à ce périmètre local (matériel et logiciel).
- **Niveaux de service :**
 - Le titulaire devra **proposer dans son offre des engagements de niveaux de service** adaptés à ce périmètre de support matériel et local (incluant le support de proximité).
- **Support de proximité :**
 - Le candidat devra s'engager sur une **présence sur site d'une journée par semaine** (modulable selon les besoins).
 - Le candidat devra :
 - Présenter le processus de demande pour interventions complémentaires hors planning
 - S'engager sur le délai de réaction pour un incident matériel bloquant
 - Confirmer sa zone de couverture géographique.
- **Prestations complémentaires :**
 - Le titulaire devra assurer, sur demande de l'EPMS, **les prestations d'achat, de paramétrage, de mise en service des nouveaux postes de travail**, et d'enrôlement dans l'environnement de gestion.
- **Sécurité et protection des postes (Antivirus / EDR / XDR) :**
 - Le titulaire assurera le maintien en condition opérationnelle de la sécurité des terminaux en s'appuyant sur l'agent Microsoft Defender for Business déployé lors du Lot 1. Aucune fourniture de licence de sécurité ou d'antivirus tiers n'est attendue dans le cadre du Lot 2
 - Il devra traiter de manière proactive toute alerte de sécurité ou dysfonctionnement de l'agent de protection remonté sur une machine.

11 Réversibilité

11.1 Objet de la réversibilité

La présente clause définit les modalités de réversibilité des services d'infogérance Microsoft 365 et Azure (Lot 2), permettant à l'EPMS de reprendre en interne ou de transférer à un nouveau titulaire l'exploitation des services, à l'issue du marché ou en cas de résiliation anticipée.

11.2 Obligations du titulaire

Le titulaire s'engage à fournir un plan de réversibilité dans un délai de 2 mois suivant la notification d'attribution du présent marché, le Titulaire remettra à l'EPMS un plan de réversibilité détaillé, incluant notamment :

- La liste exhaustive des services, données et configurations concernées ;
- Les procédures techniques de transfert (export des données, migration des configurations, etc.) ;
- Les délais et échéances pour chaque étape ;
- Les responsabilités respectives du Titulaire, du nouveau titulaire ou de l'EPMS ;
- Les coûts éventuels liés à la réversibilité.

Ce plan devra être tenu à jour annuellement ou à chaque modification significative des services.

A cet effet, le candidat indiquera dans sa réponses un modèle type et les modalités prévues pour la réversibilité.

11.3 Modalités de mise en œuvre

En cas de résiliation ou de fin de marché, le Titulaire assurera :

- La restitution intégrale des informations et configurations, dans un format exploitable et documenté ;
- L'accompagnement technique de l'EPMS ou du nouveau titulaire pendant une période de 3 mois ;
- La suppression des accès et des données en sa possession après restitution.

11.4 Garanties et pénalités

Le titulaire garantit la continuité et l'intégrité des services pendant la phase de réversibilité. Tout manquement à ses obligations pourra entraîner l'application de pénalités, selon les modalités prévues au règlement de consultation.

11.5 Confidentialité et sécurité

Les données transférées dans le cadre de la réversibilité resteront soumises aux clauses de confidentialité et de protection des données personnelles, notamment de santé, prévues au contrat.