VILLE DU BOURGET

MARCHES PUBLICS DE TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION

VILLE DU BOURGET

-*-

Service de la Commande Publique

Mairie du Bourget

65, avenue de la Division Leclerc

93350 Le Bourget Cedex

Tél: 01.48.38.82.59

Appel d'Offres Ouvert

En application des articles L. 2124-1, L. 2124-2 et R. 2161-2 à R. 2161-5, R. 2162-4 2° et R. 2162-13 du Code de la commande publique

CAHIER DES CLAUSES TECHNIQUES PARTICULIERES

INFOGERANCE ET L'EXPLOITATION DU SYSTEME D'INFORMATION : SUPERVISION/MCO, RESEAUX & SECURITE, SUPPORT UTILISATEURS POUR LES BESOINS DE LA VILLE DU BOURGET

Table des matières

1 Objet du marché

La présente consultation vise à externaliser les fonctions opérationnelles de la direction des systèmes d'information (DSI) de la collectivité. Il s'agit de confier à un ou plusieurs prestataires l'exécution des prestations nécessaires au bon fonctionnement du système d'information, tout en maintenant le pilotage stratégique, budgétaire et fonctionnel au sein de la commune.

Les objectifs généraux du présent marché sont les suivants :

- La collectivité entend garantir la continuité de service sur l'ensemble des périmètres numériques en veillant à la résilience de son infrastructure, à la fluidité des usages pour les agents publics et à la réactivité des dispositifs d'intervention.
- Le titulaire devra également accompagner la collectivité dans une démarche de rationalisation budgétaire, en particulier par une révision de l'architecture technique existante, l'optimisation de l'exploitation, la maîtrise des coûts licences et l'amélioration des outils de support et d'assistance.
- L'objectif est par ailleurs de mettre en œuvre une modernisation progressive du système d'information, adaptée aux besoins des services municipaux, tenant compte des principes de sobriété numérique, de sécurité, de fiabilité et d'interopérabilité.
- Enfin, l'ensemble du projet devra respecter les obligations réglementaires applicables à une collectivité territoriale française en matière de cybersécurité (référentiels ANSSI, PIA, PRA), de protection des données personnelles (RGPD), d'accessibilité numérique (RGAA) et de transparence (documentation, supervision, CMDB).

2 Contexte général

2.1 Présentation de la collectivité et de ses services

La Ville du Bourget, située en Seine-Saint-Denis (93) au nord-est de Paris, compte environ 17000 habitants et près de 300 agents territoriaux. Son territoire regroupe des équipements municipaux variés — écoles, équipements culturels, installations sportives, services techniques, établissements recevant du public — qui structurent un système d'information étendu et multisite au service de l'action publique locale. Les politiques publiques menées en matière d'éducation, de culture, d'urbanisme et de numérique impliquent un environnement technique fiable, sécurisé et disponible, à même de soutenir les usages quotidiens des directions et l'accueil du public.

2.2 Organisation actuelle de la DSI

La direction des systèmes d'information est aujourd'hui organisée autour d'un socle interne resserré :

- Un technicien informatique occupe un rôle d'interface opérationnelle de terrain. Il assure la supervision de premier niveau, la coordination des interventions techniques sur les sites municipaux, la remontée des incidents auprès de la DSI et des prestataires concernés, ainsi que le suivi des rétablissements jusqu'à la clôture des demandes.
- Une secrétaire assume les fonctions administratives et financières de la DSI : suivi des marchés publics en cours, préparation et traitement des commandes, rapprochement factures/prestations, tenue des tableaux de bord budgétaires et dialogue de gestion avec la direction des finances.
- Un consultant externe, mandaté par la Ville, assure le pilotage stratégique des sujets SI et la préparation/animation de la procédure de consultation relative à l'externalisation des fonctions opérationnelles. Il sert d'interface avec le maire, le cabinet, l'élu au numérique, la direction générale des services et les directions utilisatrices, arbitre les priorités, garantit la cohérence des décisions et contrôle l'exécution des prestations au plan contractuel, organisationnel et budgétaire.

À ce stade, les opérations techniques quotidiennes (exploitation de la plateforme Nutanix/AHV, gestion du VDI Citrix, sauvegardes « standards », administration des pare-feu Forcepoint, réseau et Wi-Fi Meraki) sont réalisées par des prestataires titulaires de marchés en vigueur, sous la coordination du technicien et du consultant externe, et sous la responsabilité de la DSI. Cette organisation vise à assurer la continuité de service tout en préparant la mise en concurrence et le cadrage contractuel du présent projet d'externalisation.

2.3 Cadre réglementaire et principes de gestion publique

Les prestations s'inscrivent dans le respect des référentiels et obligations applicables aux collectivités territoriales : protection des données à caractère personnel (RGPD), cybersécurité (référentiels ANSSI, PSSI, PRA/PCA), accessibilité numérique (RGAA) et transparence documentaire (traçabilité, supervision, CMDB). Sur le plan financier, la Ville veille à la soutenabilité et à la prévisibilité des dépenses dans le cadre des principes d'annualité budgétaire et de bonne gestion, en privilégiant des architectures sobres, durables et maîtrisées.

2.4 Efforts déjà réalisés et acquis structurants

La Ville a engagé, ces dernières années, plusieurs chantiers structurants de modernisation du système d'information. L'hébergement des charges de travail a été rationalisé par la mise en place d'une infrastructure hyperconvergée Nutanix à trois nœuds, supportant la virtualisation généralisée des serveurs et des services d'infrastructure. Un environnement de postes de travail virtualisés Citrix (VDI) a été déployé pour répondre aux besoins de standardisation, d'accès distant sécurisé et de continuité d'activité ; la généralisation des clients légers est en cours sur les sites éligibles.

Sur le poste de travail et la collaboration, Microsoft 365 est opérationnel (messagerie, bureautique, Teams, OneDrive). La Ville a par ailleurs privilégié le recours au SaaS pour une part significative des applications métiers (finances et RH Ciril, portails et démarches, outils de gestion documentaire et d'archives etc.), réduisant l'empreinte d'hébergement local et facilitant la mise à jour fonctionnelle.

Enfin, l'outillage ITSM GLPI est en cours de déploiement pour structurer la gestion des incidents et des demandes, la base de connaissance et le reporting des niveaux de service.

Sur le plan budgétaire, ces évolutions ont permis une première maîtrise du coût total de possession (TCO) : mutualisation des ressources par la virtualisation, externalisation ciblée des briques applicatives en mode service et contrôle des dépenses récurrentes par la standardisation des postes et la rationalisation des imprimantes autour du marché de copieurs. La Ville a, en parallèle, organisé ses approvisionnements via des centrales d'achat et marchés existants (matériels, téléphonie, liaisons intersites), afin de sécuriser les prix, les délais et la conformité.

2.5 Enjeux résiduels et axes de progrès

Malgré ces acquis, plusieurs enjeux demeurent. La rationalisation du VDI et de l'infrastructure Nutanix doit être approfondie (dimensionnement, TCO, cas d'usage pertinents), de même que la généralisation des clients légers sur les sites adaptés. A noter que l'opportunité de migrer vers un hébergement mutualisé de l'infrastructure informatique est envisageable dans le cadre du présent marché.

L'urbanisation des flux et l'interopérabilité entre applications (locales et SaaS) doivent être consolidées par une cartographie à jour et une normalisation des interfaces. La sobriété numérique constitue un axe prioritaire : optimisation des consommations (postes, serveurs, stockage, Wi-Fi), politiques d'impression responsables et allongement du cycle de vie des équipements. La réversibilité, l'éviction des dépendances techniques et la portabilité des configurations et des données restent des principes directeurs. Enfin, l'adhérence avec des environnements spécifiques (police municipale et CSU, hors périmètre d'exploitation mais interconnecté pour les usages bureautiques) appelle une attention particulière en matière de segmentation, de sécurité et de gouvernance.

2.6 Articulation avec l'écosystème de la ville

Le système d'information communal s'articule avec d'autres marchés publics en vigueur : téléphonie fixe et mobile via le SIPPEREC, copieurs via la centrale d'achat de la Région Île-de-France, liaisons inter-bâtiments en fibre dédiée et fourniture de matériels informatiques par des titulaires référencés. Le présent marché s'insère dans cet écosystème sans redondance, en privilégiant la coordination technique, la clarté des interfaces et la traçabilité des responsabilités, dans l'intérêt d'une continuité de service de qualité et d'une trajectoire de coûts maîtrisée.

3 Périmètre fonctionnel du système d'information

3.1 Typologie des utilisateurs

Le système d'information communal dessert une pluralité d'utilisateurs aux profils variés :

- Agents territoriaux : environ 200 utilisateurs actifs, répartis entre l'Hôtel de Ville, les écoles publiques, les centres culturels et médiathèques, les services techniques, ainsi que les maisons de quartier et autres lieux ouverts au public. Ces agents constituent le socle principal des utilisateurs internes de la collectivité.
- Utilisateurs partagés avec la Police municipale : des postes bureautiques sont mutualisés avec les services de police municipale (hors périmètre CSU). Ils nécessitent une gestion particulière afin d'assurer la compatibilité technique et la sécurité des interconnexions.
- Enseignants des établissements scolaires : bien que n'étant pas salariés de la Ville, les enseignants utilisent les équipements mis à disposition dans les écoles (postes informatiques, tableaux blancs interactifs, imprimantes réseau, accès Wi-Fi pédagogique). Leur bon fonctionnement relève de la responsabilité de la collectivité.
- Usagers du service public : le système d'information permet également l'accès à des postes informatiques en libre-service dans les médiathèques, centres culturels et maisons de quartier, ainsi qu'à des réseaux Wi-Fi publics. Ces usages, orientés vers l'inclusion numérique et l'accès à l'information, nécessitent une supervision spécifique afin de garantir la sécurité des connexions et la continuité de service.

Cette diversité d'utilisateurs, internes et externes, impose une approche différenciée en termes de gestion des accès, de support technique et de continuité de service, dans le respect des obligations réglementaires et des objectifs de qualité du service public.

3.2 Infrastructures techniques

3.2.1 Architecture générale et hébergement

Le système d'information s'appuie sur une infrastructure hyperconvergée Nutanix (AHV) composée de trois nœuds. Elle héberge l'essentiel des charges de travail : machines virtuelles applicatives, services d'infrastructure (AD/DNS/DHCP), partages de fichiers et bases de données. Les capacités observées à date font état d'environ 22 VM pour un cumul d'allocations visibles d'environ 102 Go de RAM et 44 vCPU (valeurs à consolider lors de l'audit de démarrage).

La haute disponibilité est assurée au niveau de la plateforme ; la Ville conserve quelques serveurs physiques résiduels pour des besoins spécifiques. L'exploitation courante est réalisée par l'infogérant, sous gouvernance de la DSI.

3.2.2 Virtualisation du poste de travail et clients légers

Un environnement VDI Citrix fournit des postes standardisés et sécurisés (accès distant, continuité d'activité, salles publiques). Environ 50 postes sont actuellement déployés ; la cible est une généralisation aux usages éligibles, avec postes virtuels à état persistant lorsque nécessaire. Le parc demeure hybride (postes Windows « lourds » + clients légers), ces derniers devant être étendus site par site après étude de compatibilité applicative, stockage et IOPS (impacts spécifiques des profils persistants).

3.2.3 Services d'infrastructure et identités

La gestion des identités repose sur Active Directory (groupes, GPO). Microsoft 365 est déployé (messagerie, collaboration) sous gouvernance DSI : authentification multi-facteur (MFA) pour certains utilisateurs, accès conditionnel.

3.2.4 Stockage, sauvegardes et continuité d'activité

Le stockage primaire est fourni par la couche HCI. Les sauvegardes actuelles, réalisées par l'infogérant sortant, sont simples et doivent être renforcées. Le titulaire mettra en place une politique ciselée par périmètre (prod/hors-prod, fichiers, configurations, Microsoft 365), visera un schéma 3-2-1 (copie externalisée, immuabilité lorsque pertinent) et des tests de restauration périodiques avec procès-verbaux. Les RPO/RTO seront fixés par famille de services et intégrés au PRA/PCA.

3.2.5 Sécurité opérationnelle et accès distants

La protection périmétrique s'appuie sur des Forcepoint NGFW 1101 administrés via NGFW Security Management Center (aujourd'hui hébergé et opéré par l'actuel titulaire). Les accès distants s'effectuent en VPN avec MFA. Les droits élevés sont limités, tracés et, le cas échéant, opérés via bastion. Les postes et certains serveurs sont protégés par une solution antivirus/EDR supervisée. Les journaux de sécurité et d'administration sont centralisés et conservés au minimum 12 mois (ou plus si obligation légale ou réglementaire), avec accès en lecture pour la DSI et le DPO.

3.3 Réseaux et interconnexions

3.3.1 Segmentation et cœur de réseau

Le réseau de la Ville est segmenté en VLAN (utilisateurs, serveurs, téléphonie, invités, administration) avec filtrage inter-segments. Le cœur/distribution s'appuie sur Cisco Meraki MS425-32 et Cisco Nexus ; l'accès est assuré par des gammes Meraki MS210/MS220/MS120 (48/24/8 ports).

3.3.2 Liaisons intersites

Les interconnexions entre bâtiments sont fournies par Ineo (fibre dédiée). Le titulaire supervise la disponibilité, la latence et les débits et coordonne les gestes opérateurs selon un plan d'interface validé par la DSI (points de contact, délais, escalade).

3.3.3 Wi-Fi interne et public

Le Wi-Fi repose sur des points d'accès Cisco Meraki, gérés en mode cloud via le Dashboard Meraki (pas de contrôleur matériel sur site). Neuf SSID sont recensés. Les usages internes seront basculés sur 802.1X (adossé NPS/AD) ; le portail captif est réservé aux invités, avec isolement L3 des flux invités, filtrage, journalisation et CGU conformes.

Accès filaires sécurisés. La mise en œuvre d'un 802.1X sur le filaire (ou NAC équivalent) est planifiée afin de renforcer l'authentification des postes et la posture de sécurité par segment.

Journalisation et conformité. Les journaux réseau et d'authentification sont centralisés et conservés 12 mois a minima (ou la durée légale supérieure si applicable), avec export mensuel vers le référentiel de la Ville.

3.4 Parc matériel et acquisition

Le parc comprend des postes fixes et portables, des clients légers, des imprimantes locales, les équipements actifs (Meraki/Nexus, Forcepoint, points d'accès) et des onduleurs (actuellement peu déployés, à renforcer sur les sites critiques).

Les acquisitions s'effectuent via les marchés existants (InMac W Store, SIPPEREC), dans le respect du Code de la commande publique.

3.4.1 Intégration et cycle de vie

Le titulaire assure :

- L'intégration matérielle (réception, installation, raccordement, étiquetage, tests),
- La préparation logicielle (master, durcissement, agents EDR/supervision, adhésion domaine),
- La mise à jour de la CMDB (numéro de série, localisation, affectation, garantie, statut, fin de vie prévisionnelle),
- Le pilotage du cycle de vie (réaffectation, réemploi interne, effacement sécurisé, sortie d'inventaire),
- L'accompagnement à la prise en main lors de la première mise à disposition.

Un plan d'équipement et de supervision des onduleurs est établi pour les baies actives et locaux techniques prioritaires (dimensionnement, télésurveillance, remplacement préventif).

3.5 Périmètre logiciel

3.5.1 Logiciels métiers

Service	Editeur	Nom	Type de déploiement
Médiathèque		Portail	SaaS
Médiathèque	Archimed	Syracuse	SaaS
Médiathèque		Electre	SaaS
Médiathèque		Neos	On premise
Enfance	Ciril	Enfance	SaaS
Finance	Ciril	Finance	SaaS
RH	Ciril	RH	SaaS
Mission Emploi	Intuition Software	Jobaffinity	SaaS
Finance	Etat	TotEM	SaaS
Finance	Financeactive	Financeactive	SaaS
CCAS	UP	Millésime	SaaS
Finance	Salvia	Salvia Patrimoine	SaaS
Finance	Docapost	Fast	SaaS
Police Municipale	Logitud	Municipol	SaaS
Police Municipale	Axone	Cam Manager	On premise
Police Municipale	Intratone	Intratone	On premise
Police Municipale	YouTransactor	Fines	SaaS
Police Municipale	Etat	AGC	SaaS
Police Municipale	Genetec	Genetec	SaaS
Police Municipale	Synchronic	PC Pass	SaaS
Police Municipale	YouTransactor	YouTransactor	SaaS
Police Municipale	Beweiss	Beweiss	On premise

Police Municipale	Synchronic	XPert Evolution	On premise
Police Municipale	Stid	Beweapon	On premise
Petite enfance	Ciril	Enfance	SaaS
Urbanisme	GFI	Cart@DS	SaaS
Urbanisme	Docapost	Certinomis	SaaS
CCAS	AFI	Pelehas	SaaS
Affaires Générales	Logitud	Suffrage web élections	SaaS
Affaires Générales	Digitech	City Web	On premise
Affaires Générales	Digitech	Logicime	On premise
Affaires Générales	Adic	Recensement	SaaS
Affaires Générales	Adic	Acte état Civil	SaaS (décomissioné)
Conservatoire	RDL	Rapsodie	SaaS
Transverse	E2time	Système de pointage	SaaS
Transverse	Kyocera	myQ	On premise
CTM	Pollux	Pollux	SaaS
CTM	Eden Innovation	Senator FX	On premise
DSI (HDV)	Til Technologies	Micro Sésame	On premise
Transverse	SRCI	IxBus	SaaS
Communication	Legalview	IPOView	SaaS
Etat Civil	Gescime	Gescime	SaaS

3.5.2 Logiciels bureautiques et transverses

3.5.2.1 Microsoft 365 (messagerie, bureautique, Teams, OneDrive)

L'environnement collaboratif de la collectivité repose sur Microsoft 365, déjà déployé. Le titulaire en assure l'administration opérationnelle (gestion des comptes, groupes et licences, accès conditionnel, authentification multi-facteur, gouvernance des partages, rétention et audit), sous le contrôle de la DSI. La ville conserve la pleine maîtrise du tenant, des habilitations stratégiques et des décisions de configuration. Toute évolution de paramétrage est proposée par le titulaire et validée préalablement par la DSI.

3.5.2.2 GLPI (ITSM)

GLPI est en cours de déploiement et sera l'outil central de gestion des demandes et incidents, de la base de connaissance, de l'inventaire et du reporting SLA. Le titulaire exploite l'outil au quotidien et peut proposer des reparamétrages fonctionnels ou techniques, après validation de la DSI. L'application et l'intégralité de ses données demeurent dans le périmètre de la ville (propriété, administration de haut niveau, sauvegardes, réversibilité).

3.5.2.3 Suites créatives Adobe sur Mac (service communication)

Le service communication utilise des postes Mac équipés des suites Adobe. Le titulaire assure le support technique et le maintien en condition opérationnelle (mises à jour macOS et applicatives, compatibilité réseau et sécurité, intégration à l'annuaire et aux services collaboratifs), avec un niveau de qualité de service équivalent aux autres postes de la collectivité.

3.5.2.4 Certificats numériques (Certinomis)

Les certificats numériques transverses (SSL/TLS, messagerie, authentification, signature) sont délivrés via Certinomis. Le titulaire tient à jour l'inventaire, supervise les échéances, procède aux renouvellements sans interruption de service, sécurise les clés privées et met à jour la documentation associée, en cohérence avec la PSSI de la ville et les recommandations de l'ANSSI.

3.5.2.5 Antivirus/EDR

L'ensemble des postes et serveurs est protégé par une solution antivirus/EDR. Le titulaire en assure le déploiement, la mise à jour des moteurs et politiques, la supervision des alertes, le traitement des incidents de sécurité selon les procédures établies et la production de rapports réguliers à la DSI (taux de couverture, événements, remédiations).

3.5.2.6 Parapheur électronique IXBus (SRCI)

La collectivité dispose d'un parapheur IXBus édité par SRCI. Le titulaire en assure l'exploitation technique courante (paramétrages, mises à jour, supervision, sauvegardes), la gestion des interconnexions nécessaires (annuaire, messagerie, éventuellement SSO) et la tenue d'une documentation à jour, dans le respect des exigences de sécurité, de traçabilité et de protection des données applicables aux organismes publics.

3.6 Sites spécifiques

Le titulaire assure le maintien en conditions opérationnelles (MCO), la sécurité et la supervision des équipements et services numériques de l'ensemble des sites municipaux listés ci-après. Il veille à l'homogénéité des configurations (réseau, Wi-Fi, authentification, sauvegardes), au respect des politiques de sécurité et à l'actualisation de la CMDB à chaque évolution (déplacement, ouverture/fermeture de site, ajout d'équipements). Les interfaces avec les tiers (opérateurs, exploitants dédiés) sont coordonnées via un plan d'interface approuvé par la DSI.

- **Livrables :** fiche « site » normalisée (adresse, contacts, raccordements, VLAN/SSID, équipements actifs, onduleurs, …), plan des baies, plan de numérotation/ports, résultats de tests, procédures locales d'exploitation, mise à jour CMDB.
- **Critères :** isolement L3 entre réseaux internes et invités validés ; couverture Wi-Fi conforme au plan ; supervision active sur 100 % des actifs recensés ; restauration d'un poste type « école » et « accueil public » réalisable selon procédure ; conformité aux obligations de conservation/journalisation sur les sites avec Wi-Fi public et/ou vidéoprotection (cf. autorisations préfectorales et recommandations CNIL).

3.6.1 Administration centrale

- Hôtel de ville
- Centre communal d'action sociale (CCAS)
- Centre technique municipal
- Cimetière

Exigences communes : sécurisation des baies (onduleurs, contrôle d'accès), segmentation réseau par VLAN (bureautique, téléphonie, invités), couverture Wi-Fi interne, postes d'accueil du public si présents et continuité des services métiers (état civil, finances, RH).

3.6.2 Education et petite enfance

Ecoles primaires : école Jacqueline Auriol, école Jean Jaurès, école Jean Mermoz, école Louis-Blériot, école Saint-Exupéry.

Petite enfance : crèche Maryse Bastié (structure collective \~65 berceaux), halte-jeux la petite escadrille, relais petite enfance « la caravelle » (accueil et informations aux familles et assistants maternels).

Exigences spécifiques : postes enseignants, TBI, imprimantes réseau, Wi-Fi pédagogique distinct et filtré, conformité aux chartes académiques lorsque requis. Le titulaire assure la maintenance et l'évolution des parcs, la gestion des profils et des restrictions d'accès, ainsi que la supervision des réseaux locaux des écoles.

3.6.3 Culture, lecture publique et enseignements artistiques

- Médiathèque « le point d'interrogation » (service de lecture publique au centre-ville).
- Centre culturel André Malraux (programmation culturelle et services aux usagers).
- Conservatoire du Bourget (musique, danse, art dramatique).

Exigences spécifiques : postes en libre accès public (médiathèque), Wi-Fi public avec journalisation légale, filtrage des flux et isolement strict des réseaux invités ; continuité des postes d'accueil/billetterie et des systèmes métiers (gestion documentaire, portails culturels).

3.6.4 Sports et équipements ouverts au public

Espace éducatif et sportif Maurice Houyoux (complexe sportif municipal), équipements attenants (Stade Roger Salengro).

Piscine du Bourget (bassin couvert, activités aquatiques).

Exigences spécifiques : couverture Wi-Fi adaptée au public et aux usages internes, disponibilité des postes d'accueil et de contrôle, segmentation des réseaux entre billetterie, exploitation et invités ; surveillance de la qualité de service dans les lieux à forte fréquentation.

3.6.5 Services de proximité et hébergement seniors

- Résidence autonomie « Aline Marlin »
- Relais petite enfance
- Autres sites de proximité : maisons de quartier, équipements associatifs le cas échéant.

Exigences spécifiques : prise en compte de postes partagés, profils multi-utilisateurs, impression sécurisée, Wi-Fi invité isolé lorsque présent.

3.6.6 Police municipale et vidéoprotection urbaine (adhérence)

La police municipale opère un système d'information dédié et un centre de supervision urbaine (CSU) dont l'exploitation reste hors périmètre du présent marché (prestataire actuel : Bouygues Services). Toutefois, les postes bureautiques de la police municipale, interconnectés au réseau communal pour les usages courants, sont inclus dans le MCO et le support.

Adhérence et convergence des socles : le titulaire veille à la compatibilité technique (annuaire, messagerie, sécurité poste), à la segmentation réseau et à la sécurité des interconnexions. Une convergence progressive des socles techniques (poste, authentification, sécurité) est recherchée, sans préjudice de l'autonomie opérationnelle du CSU.

3.6.7 Evolutions patrimoniales et nouveaux sites

Le périmètre du marché couvre également les projets immobiliers à venir (création de nouveaux équipements, extensions, déménagements, réaménagements). Le titulaire :

- Réalise les études techniques préalables (raccordements réseau/fibre, baies et onduleurs, Wi-Fi, sûreté, postes),
- Propose un chiffrage et un planning d'intégration (dont livraison de la documentation et mise à jour de la CMDB),
- Coordonne les interfaces avec les prestataires tiers (Ineo pour les liaisons fibre, SFR Business pour la téléphonie, Kyocera pour l'impression, Bouygues Services pour les dépendances avec le CSU),
- Remet un PV de recette par site (tests réseau/Wi-Fi, accès aux applications, supervision, sauvegardes le cas échéant).

4 Structure des prestations et tranches du marché

4.1 Tranche ferme 1 – Refonte et sécurisation de l'infrastructure

4.1.1 Audit initial détaillé de l'existant (infrastructure, réseaux, interconnexions, systèmes, stockage, licences)

Le titulaire mènera, dès le démarrage du marché, un audit initial exhaustif de l'ensemble du système d'information existant de la collectivité. Cette mission a pour objet de fournir une cartographie précise, documentée et à jour des infrastructures, des systèmes et des logiciels en place, en vue de faciliter la reprise d'exploitation et de proposer les actions de rationalisation et d'optimisation les plus pertinentes.

L'audit portera sur les équipements matériels (serveurs, postes de travail, périphériques, équipements réseaux), les infrastructures virtualisées (Nutanix, Citrix etc.), les interconnexions entre sites (liaisons fibre, VLAN, VPN), les dispositifs de sécurité (pare-feu, antivirus, systèmes de sauvegarde), les outils de supervision, les certificats et mécanismes d'authentification, les licences logicielles (types, modes de déploiement, renouvellement), les flux applicatifs critiques, ainsi que l'état des documentations disponibles. Il prendra également en compte les contraintes techniques propres aux logiciels métiers, qu'ils soient hébergés en local ou en SaaS.

L'ensemble des constats fera l'objet d'un rapport d'audit détaillé, remis à la collectivité sous forme écrite et présenté oralement lors d'une réunion de restitution. Ce rapport devra proposer une analyse critique, structurée par périmètre fonctionnel, accompagnée d'un inventaire, d'une analyse de conformité réglementaire (cybersécurité, RGPD) et d'un ensemble de recommandations opérationnelles pour fiabiliser, moderniser et rationaliser l'infrastructure et les usages numériques de la commune.

4.1.2 Rationalisation de toute l'infrastructure hébergée sur Nutanix, incluant le VDI (étude TCO complète, scénarios techniques, plan d'optimisation, migration partielle ou totale)

Le titulaire procédera à une rationalisation complète de l'infrastructure virtuelle actuellement hébergée sur la plateforme Nutanix, incluant l'environnement de virtualisation des postes de travail (VDI) sous Citrix. Cette démarche visera à évaluer, optimiser et éventuellement transformer l'architecture technique en place dans une logique de maîtrise budgétaire, de performance opérationnelle et de soutenabilité à moyen terme.

L'intervention du titulaire débutera par une étude complète du coût total de possession (TCO) intégrant l'ensemble des composantes matérielles et logicielles, les coûts d'exploitation, de maintenance, de licences, ainsi que les charges indirectes. Cette étude devra comparer plusieurs scénarios techniques, notamment le maintien de l'existant, la migration partielle vers une solution alternative, ou la réversibilité totale vers une infrastructure externalisée ou hybride.

Sur la base de cette analyse, le titulaire proposera un plan de transformation détaillé, hiérarchisé et chiffré, tenant compte des contraintes techniques de la collectivité, de l'éligibilité à d'éventuels financements publics (plan France Relance, fonds DETR etc.) et des exigences de continuité de service. Ce plan précisera les étapes de migration ou d'adaptation (techniques, organisationnelles, contractuelles), les ressources nécessaires, les risques associés, ainsi que les mesures d'accompagnement au changement pour les agents concernés.

La rationalisation devra également intégrer une revue des modalités d'usage du VDI afin d'en optimiser le dimensionnement, le mode de consommation et les cas d'usage pertinents (nomadisme, sécurité, accessibilité). Les recommandations du titulaire devront concourir à l'atteinte des objectifs de sobriété numérique, tout en garantissant la robustesse du système d'information communal.

4.1.3 Déploiement complet des clients légers (planification, intégration, configuration)

Le titulaire assurera le déploiement complet des clients légers sur l'ensemble des sites de la collectivité identifiés comme techniquement et fonctionnellement adaptés à ce mode de poste de travail. Cette opération s'inscrit dans une logique de rationalisation du parc informatique, de réduction des coûts de maintenance et de consommation énergétique et de sécurisation des environnements de travail.

Ce déploiement comprendra la planification détaillée des opérations site par site, en coordination avec les services utilisateurs et la direction des systèmes d'information, afin de garantir une continuité de service optimale. Il inclura la livraison, l'installation physique, la configuration initiale, le raccordement réseau, la connexion aux serveurs de publication (VDI Citrix) ainsi que les tests de bon fonctionnement.

Le titulaire devra également veiller à l'intégration des clients légers dans la supervision centralisée (CMDB, outils de monitoring), à la documentation des interventions et à l'accompagnement des utilisateurs en phase de prise en main. Le remplacement progressif des postes lourds par des clients légers devra être conduit de manière fluide, avec une attention particulière portée à la compatibilité applicative, notamment pour les logiciels métiers à contrainte technique spécifique.

4.1.4 Coordination avec les prestataires tiers (Kyocera, SFR Business, Ineo, InMac, Bouygues Services)

Le titulaire assurera la coordination opérationnelle avec les prestataires tiers exerçant des responsabilités sur des pans spécifiques du système d'information de la commune.

Il s'agit notamment de :

- Kyocera, en charge des copieurs dans le cadre du marché de la centrale d'achat de la région Île-de-France,
- SFR Business, titulaire du marché téléphonie via le SIPPEREC,
- Ineo, responsable des liaisons fibre intersites,
- InMac WStore, fournisseur référencé pour le matériel informatique dans le cadre d'un marché distinct,
- Bouygues Services, prestataire exploitant le centre de supervision urbaine (CSU).

Cette coordination vise à assurer la continuité de service, éviter les conflits d'intervention, garantir la cohérence technique des actions réalisées sur les infrastructures partagées et fluidifier les échanges d'information. Le titulaire devra ainsi mettre en œuvre des procédures de suivi et de partage d'information avec ces tiers, établir des points de contact, organiser les remontées d'incidents conjoints et participer aux éventuelles revues de service lorsque des actions croisées sont nécessaires. Il veillera en outre à documenter toutes les interactions avec ces prestataires dans les outils de pilotage de la collectivité.

4.1.5 Gestion des certificats numériques

La gestion des certificats numériques constitue un volet essentiel de la sécurité des systèmes d'information de la collectivité. Le titulaire devra assurer l'administration complète de l'infrastructure à clés publiques (PKI), qu'elle soit interne ou externalisée, en conformité avec les normes en vigueur et les exigences de l'ANSSI.

Cela implique la tenue à jour d'un inventaire exhaustif des certificats utilisés par les systèmes, applications et équipements de la ville, incluant notamment les certificats SSL/TLS des sites web, les certificats de messagerie, les certificats machine pour les connexions VPN ou réseau, ainsi que les certificats d'authentification utilisateurs ou de signature électronique. Le titulaire sera chargé de leur renouvellement dans les délais impartis, en anticipant les échéances critiques afin d'éviter toute interruption de service.

Il devra également maintenir une documentation rigoureuse et actualisée relative aux processus de gestion des certificats : procédures d'émission, de révocation, de sauvegarde, de rotation et d'audit. Une attention particulière devra être portée à la sécurisation des clés privées, au stockage des certificats dans les infrastructures techniques concernées (serveurs, équipements réseau, plateformes SaaS) et à la traçabilité des opérations effectuées. Le titulaire veillera à intégrer ces informations dans la CMDB et à en assurer la supervision continue à l'aide des outils existants ou à proposer.

Les certificats émis via Certinomis sont inventoriés, supervisés et renouvelés par le titulaire ; toute évolution d'AC ou de périmètre est proposée à la DSI.

4.2 Tranche ferme 2 – Exploitation des infrastructures et du socle numérique

4.2.1 Reprise d'exploitation progressive de l'ensemble des composants techniques

Le titulaire procédera à la reprise d'exploitation progressive de l'ensemble des composants techniques du système d'information de la collectivité. Cette phase, essentielle à la continuité de service, devra permettre de reprendre la main sur les environnements techniques existants en garantissant leur bon fonctionnement, leur stabilité et leur conformité avec les exigences de sécurité et de performance de la collectivité.

La reprise comprendra notamment l'appropriation des systèmes virtualisés (Nutanix, Citrix), des réseaux (commutateurs, routeurs, VLAN, pare-feu), des systèmes de sauvegarde, des équipements Wi-Fi, ainsi que des services annexes tels que les annuaires, les mécanismes d'authentification et les outils de supervision. Le titulaire devra établir un plan de reprise séquencé, validé par la collectivité, permettant une transition fluide sans interruption de service, en coordination étroite avec les intervenants existants.

Cette reprise sera également l'occasion de vérifier et ajuster les configurations, de documenter les environnements dans la CMDB, d'identifier les points de fragilité ou de dette technique et de consolider les habilitations, rôles et responsabilités. Le prestataire devra mobiliser les outils et ressources adaptés pour sécuriser la continuité des opérations, tout en inscrivant son action dans une logique de transparence et de transférabilité, conformément aux obligations de réversibilité prévues au marché.

4.2.2 Supervision temps réel des infrastructures (serveurs, réseau, VDI, sauvegardes)

La supervision temps réel des infrastructures constitue un levier essentiel pour garantir la continuité de service, la réactivité opérationnelle et le respect des engagements de disponibilité pris par la collectivité. Le titulaire devra assurer un suivi permanent et structuré de l'ensemble des composants techniques du système d'information, incluant notamment les serveurs physiques et virtualisés, les équipements réseau (commutateurs, routeurs, pare-feu), l'environnement de virtualisation des postes (VDI), les solutions de stockage et les dispositifs de sauvegarde.

Cette supervision devra permettre la détection précoce des anomalies, des saturations, des indisponibilités partielles ou totales et déclencher des alertes vers les intervenants compétents conformément aux niveaux de service définis dans le marché. Elle s'appuiera sur des outils de monitoring éprouvés, en capacité de collecter, corréler et historiser les données de fonctionnement, tout en produisant des tableaux de bord accessibles à la collectivité.

La supervision inclura également la surveillance des ressources critiques (consommation CPU, mémoire, espace disque, état des processus), la disponibilité des services applicatifs hébergés localement ou dans le cloud, ainsi que la traçabilité des événements de sécurité. Le prestataire veillera à intégrer cette supervision dans l'outillage existant ou à proposer une solution cohérente, en assurant une interopérabilité avec la CMDB, un archivage des incidents et une capacité de reporting adaptée aux exigences de pilotage des collectivités territoriales.

4.2.3 Maintenance préventive et curative (serveurs, réseau, postes, sauvegardes, Wi-Fi, sécurité)

Le titulaire sera chargé d'assurer la maintenance préventive et curative de l'ensemble des composants techniques du système d'information de la commune. Cela inclut les serveurs physiques et virtualisés, les équipements réseau (commutateurs, routeurs, pare-feu), les postes de travail fixes et mobiles, les dispositifs de sauvegarde de données, ainsi que les infrastructures Wi-Fi internes et publiques.

La maintenance préventive comprendra la réalisation régulière d'opérations de vérification, de nettoyage, de mise à jour, de test de performance et de contrôle de sécurité sur l'ensemble des équipements et services concernés, selon un calendrier validé en début de marché. L'objectif est de prévenir les incidents, d'anticiper les dysfonctionnements et de garantir un fonctionnement optimal du système d'information.

La maintenance curative interviendra en cas de panne, d'incident ou de dégradation du service. Elle devra être déclenchée selon des modalités précisées dans les engagements de niveau de service (SLA), avec des délais d'intervention adaptés à la criticité des composants concernés. Le titulaire devra documenter chaque intervention dans la CMDB, identifier les causes racines des incidents, proposer des actions correctives durables et en rendre compte à la DSI lors des revues de service.

En matière de sécurité, le titulaire assurera le maintien en condition de sécurité des équipements et logiciels, notamment via l'application des correctifs de sécurité, le renouvellement des certificats, la surveillance des journaux d'événements et la coordination avec les éditeurs ou prestataires spécialisés. Il participera également à l'amélioration continue de la posture de cybersécurité de la collectivité, en lien avec les référentiels ANSSI et les politiques internes de sécurité des systèmes d'information.

4.2.4 Intégration et mise à jour continue de la CMDB (matériel, licences, certificats, topologie, dépendances)

Le titulaire assurera l'intégration initiale puis la mise à jour continue de la base de données de gestion de configuration (CMDB) de la collectivité. Celle-ci devra recenser de manière exhaustive et structurée l'ensemble des composants du système d'information : équipements matériels (serveurs, postes, périphériques), licences logicielles (typologie, durée, éditeur, périmètre couvert), certificats numériques (type, usage, date d'expiration, autorité de certification), topologie du réseau (VLAN, interconnexions, flux) ainsi que les dépendances techniques entre les différents éléments (relation applicative, hébergement, supervision etc.).

Le prestataire devra mettre en œuvre des procédures rigoureuses permettant de garantir la fiabilité, la traçabilité et l'exploitabilité de ces données, dans un objectif de pilotage, de supervision et de conformité réglementaire. Chaque évolution du système d'information (ajout, modification ou suppression d'un composant) devra être systématiquement enregistrée dans la CMDB avec les métadonnées associées. Le titulaire veillera à assurer l'interopérabilité de cet outil avec les autres briques logicielles de la collectivité (GLPI, outils de supervision, portail de reporting) et en garantira l'accès en lecture aux agents désignés de la direction des systèmes d'information.

4.2.5 Administration Microsoft 365 (gestion des utilisateurs, sécurité, conformité)

L'administration de l'environnement Microsoft 365 constitue une composante essentielle du système d'information de la collectivité. Le titulaire sera chargé de la gestion centralisée des

comptes utilisateurs, incluant la création, la modification, la suppression et la gestion des droits d'accès en fonction de l'organigramme communal, des mouvements de personnel et des règles d'habilitation définies par la direction des systèmes d'information.

Il devra également assurer le paramétrage et le suivi des politiques de sécurité de la suite Microsoft 365 (authentification multi-facteur, gestion des accès conditionnels, supervision des tentatives d'intrusion, surveillance des journaux d'événements) en cohérence avec la politique de sécurité des systèmes d'information (PSSI) de la ville. Une attention particulière devra être portée à la protection des données personnelles et aux dispositifs de conformité réglementaire (préservation des journaux, plans de conservation, auditabilité).

Le titulaire assurera en outre la gestion des groupes de distribution, des partages réseau, OneDrive, des canaux Teams, ainsi que des autorisations sur SharePoint et les bibliothèques documentaires associées. Il devra enfin mettre en œuvre des mesures de supervision continue, produire des rapports d'usage et de sécurité et conseiller la collectivité sur les évolutions à opérer pour garantir l'optimisation, la sécurité et la conformité de l'environnement Microsoft 365, dans une logique de service public numérique sécurisé et résilient.

4.2.6 Maintenance et supervision des Wi-Fi internes et publics

Le titulaire assurera la maintenance et la supervision des réseaux Wi-Fi internes (réservés aux agents et aux équipements métiers) ainsi que des réseaux Wi-Fi publics déployés sur plusieurs sites municipaux. Cette mission implique une surveillance active de la qualité de service, de la disponibilité des accès et du bon fonctionnement des équipements actifs (bornes Wi-Fi, contrôleurs, points d'accès).

Le prestataire veillera au maintien en condition opérationnelle des infrastructures Wi-Fi, incluant l'application des mises à jour logicielles et de sécurité, la vérification des configurations, la gestion des canaux et de la charge réseau, ainsi que la résolution rapide des incidents signalés par les utilisateurs ou détectés par les outils de supervision.

Il devra par ailleurs garantir une segmentation stricte entre les flux internes et publics afin d'assurer la sécurité des données du système d'information communal. Une attention particulière sera portée à la conformité aux exigences réglementaires (notamment RGPD), à la traçabilité des connexions sur les réseaux ouverts au public et à l'intégration des éléments supervisés dans la CMDB et les tableaux de bord de pilotage de la DSI. Le titulaire pourra être sollicité pour des extensions ou adaptations du réseau Wi-Fi dans le cadre de projets municipaux, après étude et validation technique préalable.

4.3 Tranche ferme 3 – Support aux utilisateurs et logiciels métiers

4.3.1 Support utilisateurs multicanal (tickets GLPI, téléphone, prise en main à distance, interventions N1 à N3)

Le titulaire assurera un dispositif de support utilisateurs multicanal, adapté aux besoins d'une collectivité territoriale. Ce dispositif comprendra l'accueil et le traitement des sollicitations via différents canaux : système de gestion des demandes informatiques (GLPI), assistance téléphonique, prise en main à distance sécurisée, ainsi que le cas échéant, des interventions physiques sur site.

Les interventions devront être structurées selon les niveaux de support classiquement reconnus dans le domaine des systèmes d'information :

- Niveau 1 (N1) : accueil des demandes, résolution des incidents courants, assistance à l'usage des outils bureautiques, escalade si nécessaire ;
- Niveau 2 (N2) : traitement des incidents techniques nécessitant une compétence approfondie sur les environnements métiers ou techniques ;
- Niveau 3 (N3) : expertise spécifique ou intervention en lien avec les éditeurs, les constructeurs ou les opérateurs tiers.

Le titulaire devra mettre en œuvre un suivi rigoureux des tickets ouverts, avec une priorisation selon la criticité des incidents, un engagement sur les délais d'intervention et de résolution (SLA) et une traçabilité complète dans l'outil GLPI. Il veillera à fournir une assistance accessible, pédagogique et conforme aux principes de qualité du service public, en coordination étroite avec la direction des systèmes d'information.

4.3.2 Exploitation quotidienne de GLPI (gestion des tickets, base de connaissance, reporting SLA)

Le titulaire assurera l'exploitation quotidienne de la solution GLPI, outil central de gestion des services informatiques (ITSM) de la collectivité. Cette exploitation comprend la gestion rigoureuse des tickets d'incidents et de demandes, depuis leur création jusqu'à leur résolution ou clôture, en veillant au respect des délais d'intervention et de résolution définis dans les niveaux de service (SLA).

Le titulaire aura également la charge de l'alimentation et de la maintenance de la base de connaissance, en y intégrant les procédures de résolution récurrentes, les bonnes pratiques, les consignes techniques internes et toute documentation utile à la résolution autonome des incidents ou à la montée en compétence des agents.

En complément, le prestataire devra produire des reportings réguliers à partir des données de GLPI. Ces rapports, partagés avec la direction des systèmes d'information, devront permettre un pilotage opérationnel éclairé des activités de support : volume et typologie des tickets, temps de traitement, récurrence des incidents, niveaux de satisfaction etc. Ils contribueront au suivi des engagements contractuels et à l'amélioration continue du service rendu aux agents territoriaux.

4.3.3 Support spécifique aux utilisateurs Mac (Adobe, configurations réseau, sécurité)

Le titulaire devra assurer un support technique adapté aux utilisateurs du service communication, équipés d'ordinateurs Apple Mac fonctionnant avec la suite Adobe. Cette

population d'utilisateurs présente des spécificités matérielles et logicielles qui exigent une maîtrise des environnements macOS, ainsi qu'une capacité à assurer la compatibilité des équipements avec l'infrastructure réseau de la collectivité.

Ce support inclura l'assistance à l'usage courant des outils Adobe Creative Cloud, la gestion des incidents liés aux configurations spécifiques des Mac, la mise à jour régulière des systèmes d'exploitation macOS, ainsi que la garantie de leur intégration sécurisée dans le système d'information municipal. Le prestataire devra également prendre en compte les aspects de sécurité propres à cet environnement, en veillant notamment à la conformité des configurations réseau, au respect des politiques d'authentification et à la protection des données traitées sur ces postes.

Cette mission devra être menée en étroite coordination avec la direction des systèmes d'information, en veillant à la traçabilité des interventions, à la remontée des difficultés éventuelles et à la préservation d'une qualité de service équivalente à celle fournie aux autres agents de la collectivité, dans le respect des objectifs d'harmonisation, de continuité et d'accessibilité numérique.

4.3.4 Coordination technique des logiciels métiers (incidents techniques, mises à jour, interactions avec éditeurs, hors formation et support métier)

La coordination technique des logiciels métiers relève d'une responsabilité structurante dans l'organisation du système d'information communal. Elle inclut la gestion des incidents techniques affectant les applications métiers, qu'ils soient ponctuels ou récurrents, ainsi que la supervision des opérations de maintenance applicative telles que les mises à jour correctives ou évolutives. Le titulaire assurera l'interface technique avec les éditeurs et prestataires concernés, qu'il s'agisse de solutions hébergées en SaaS, de logiciels installés sur les infrastructures de la collectivité ou d'applications en environnement hybride.

Il veillera à organiser, en lien avec la direction des systèmes d'information, un suivi actif des versions logicielles, des cycles de mise à jour et des prérequis techniques, afin d'anticiper toute rupture de service ou toute incompatibilité avec l'environnement technique de la collectivité. Il pourra être amené à participer à des comités de suivi avec les éditeurs, à assurer la validation technique de nouvelles versions avant déploiement, ou à mettre en œuvre des procédures de retour arrière le cas échéant.

Cette mission ne couvre pas la formation des agents ni le support métier proprement dit, qui restent de la responsabilité des directions fonctionnelles utilisatrices. Elle s'inscrit toutefois dans un rôle de coordination technique, garantissant l'efficience, la résilience et la cohérence du parc applicatif métier au service des politiques publiques locales.

4.4 Tranche conditionnelle 1 – Sobriété numérique

4.4.1 Objet et périmètre

La tranche a pour objet d'objectiver l'empreinte environnementale du système d'information communal et de déployer des mesures concrètes de réduction, sans dégrader la qualité de service rendu aux usagers et aux agents. Elle couvre le poste de travail (y compris clients légers), les serveurs et services hébergés, le VDI, les impressions, les stockages et sauvegardes, les réseaux et le Wi-Fi, ainsi que les services numériques externes (SaaS) lorsque la Ville est responsable du paramétrage et des usages. Les actions sont conduites en cohérence avec les orientations de la DSI, la PSSI, le RGPD et les règles budgétaires de la collectivité.

4.4.2 Diagnostic complet des usages (postes, serveurs, impressions, stockage)

Le titulaire réalise un état des lieux exhaustif, quantifié et cartographié :

- Poste de travail : typologie des matériels, taux d'usage réel, profils énergétiques, politiques de mise en veille/arrêt, applications en démarrage automatique, cycle de vie et taux de réemploi.
- Serveurs/VDI : consolidation des charges (CPU, RAM, I/O), taux de virtualisation, densité VMs/nœud, bonnes pratiques d'ordonnancement et d'extinction planifiée des environnements non-productifs.
- Impressions : volumes par site et par service, recto-verso et N&B par défaut, authentification/libération de travaux (myQ/Kyocera), localisation des copieurs, impressions orphelines.
- Stockage et sauvegardes : volumétrie par espace et par application, taux de doublons, données dormantes/chaudes, politique de rétention, compression/déduplication, externalisation.
- Réseaux/Wi-Fi : profils d'activité, charge moyenne/heure de pointe, optimisation des puissances d'émission et du nombre de bornes actives hors horaires.

Le diagnostic distingue gains « sans investissement » immédiats (réglages, politiques, scripts) et gains avec investissement (renouvellements, réarchitecturations) et s'appuie sur des mesures outillées (supervision, GLPI/CMDB, relevés de consommation lorsque disponibles).

4.4.3 Analyse énergétique de l'infrastructure existante

Le titulaire établit une analyse énergétique structurée par périmètre : postes, VDI/Nutanix, stockage/sauvegardes, réseau/Wi-Fi, impression, locaux techniques. Il calcule des indicateurs de référence (kWh/an, W/poste, W/VM, kWh/page, kWh/AP Wi-Fi, PUE ou équivalent lorsque pertinent) et identifie les gisements d'économie. Lorsque les données directes ne sont pas disponibles, il propose une méthode d'estimation fondée sur des facteurs publiés et la consolide au fil des mesures.

4.4.4 Plan d'actions de réduction (migration, arrêt d'équipements, optimisation de postes, politiques d'impression)

Sur la base du diagnostic, le titulaire propose une trajectoire pluriannuelle priorisée, chiffrée (coûts/économies) et jalonnée :

- Optimisation poste de travail : mise en veille/arrêt forcés par GPO/MDM, rationalisation des agents en démarrage, déploiement ciblé de clients légers, allongement du cycle de vie, réemploi interne, effacement sécurisé et don/valorisation des DEEE via filières agréées.
- Rationalisation serveurs/VDI : densification, extinction planifiée des environnements de recette/hors-prod, ajustement des images VDI, réduction du nombre de masters, scénarios de démarche « arrêt quand inutile » (hors heures, week-ends) lorsque compatible avec les usages.
- Stockage et sauvegardes : politiques d'archivage/retenue différenciées, déduplication, suppression des doublons, nettoyage des espaces partagés, conservation légale maîtrisée, bascule progressive vers un schéma 3-2-1 avec copie externalisée immuable.
- Impressions : recto-verso/N&B par défaut, quotas par service, suppression des imprimantes locales isolées, relocalisation des copieurs, généralisation de l'authentification/libération, sensibilisation des agents (tableaux de bord de consommation).
- Réseaux/Wi-Fi : plan d'extinction/abaissement de puissance hors horaires sur sites éligibles, nettoyage des SSID redondants, revue des politiques d'échantillonnage et de logs pour limiter les volumes superflus.

Chaque action précise les impacts attendus, les risques et la marche à suivre (procédures, réversibilité, communication agent).

4.4.5 Livrables attendus

- Rapport de diagnostic (état des lieux, mesures, indicateurs de référence).
- Dictionnaire des leviers de sobriété par périmètre, avec prérequis techniques et organisationnels.
- Plan d'actions priorisé (gains estimés, CAPEX/OPEX, planning, dépendances, risques).
- Kits de mise en œuvre : GPO/MDM types, scripts, modèles de politiques d'impression, procédures d'archivage/nettoyage.
- Tableaux de bord (mensuels puis trimestriels) : consommation, gains réalisés, alertes et dérives, actions en cours.
- PV de recette des mesures appliquées (tests, relevés, validation DSI).

4.4.6 Critères de recette et indicateurs

Ces valeurs sont données à titre indicatif et devront être déterminées avec le titulaire lors du recours à la présente tranche du marché :

- Poste de travail : ≥ 90 % des postes avec mise en veille auto < 15 min et arrêt auto en dehors des plages définies ; baisse de 15–25 % de la consommation moyenne par poste à 12 mois.
- Serveurs/VDI : extinction/horaire des environnements non-productifs appliquée sur ≥ 80 % des cas éligibles ; densité VM/nœud améliorée de 10–20 % sans dégradation des SLA.
- Stockage : réduction de 20–30 % des doublons/volumétrie « froide » sur les partages ciblés ; rétention différenciée documentée et appliquée.
- Impressions : −30 % de pages A4/an par rapport à l'année N-1 sur les périmètres ciblés ; ≥ 95 % des travaux en recto-verso et N&B par défaut.
- Réseaux/Wi-Fi : plan d'extinction/abaissement en heures creuses mis en œuvre sur tous les sites éligibles, sans incident de service.
- Reporting : tableaux de bord validés en comité de pilotage, données tracées dans GLPI/CMDB lorsque pertinent.

4.4.7 Pilotage, communication et accompagnement au changement

La mise en œuvre est suivie en comité de pilotage sobriété (DSI, directions utilisatrices, titulaire). Le titulaire fournit supports de communication interne, fiches pratiques et sessions courtes de sensibilisation des agents. Les changements potentiellement impactants (ex. politiques d'impression) font l'objet d'une information préalable et d'une période d'observation avec retour d'expérience.

4.4.8 Articulation contractuelle et budgétaire

Les actions « sans investissement » et les reparamétrages relèvent de la présente tranche (forfait) ; les remplacements matériels ou évolutions structurantes sont proposés avec chiffrage (BPU/DQE ou avenant selon le cas), en respectant les principes d'annualité et de prévisibilité budgétaire.

Les interactions avec les marchés tiers (Kyocera pour les copieurs, SIPPEREC/SFR Business pour la téléphonie, Ineo pour les liaisons) sont coordonnées pour éviter toute redondance et maximiser les gains.

5 Obligations générales du titulaire

5.1 Garantie de continuité de service

Le titulaire du marché est contractuellement tenu d'assurer, en toutes circonstances, la continuité des services numériques de la collectivité. Cette exigence centrale implique le respect strict des engagements de niveau de service (Service Level Agreement - SLA) fixés dans les documents contractuels, couvrant notamment les délais de rétablissement des services, les plages de disponibilité des ressources et la qualité des prestations rendues aux utilisateurs finaux.

5.2 Suivi opérationnel

Afin de garantir cette continuité, le titulaire mettra en œuvre un dispositif de suivi opérationnel structuré. Ce dispositif comprendra l'organisation de comités de pilotage mensuels associant

les représentants de la collectivité et les responsables opérationnels du titulaire. Ces comités auront pour mission d'examiner les indicateurs de performance (KPI), de suivre les alertes critiques ou récurrentes, d'analyser les éventuels écarts par rapport aux SLA et de proposer les mesures correctives nécessaires. Des tableaux de bord consolidés seront produits régulièrement et mis à disposition de la direction des systèmes d'information.

5.3 Coopération avec les équipes internes

Le prestataire devra entretenir une coopération fluide avec les équipes internes de la collectivité, qu'il s'agisse des agents de la DSI, des directions fonctionnelles, ou des référents techniques identifiés dans les différents services municipaux. Il est attendu une posture proactive, fondée sur la transparence, la réactivité et la mise en place de circuits de communication efficaces, notamment en cas d'incident majeur ou de changement planifié.

5.4 Sécurité, confidentialité et résilience

Le titulaire est tenu de respecter l'ensemble des exigences réglementaires et contractuelles en matière de protection des données à caractère personnel (RGPD), de cybersécurité (référentiels ANSSI, mesures techniques et organisationnelles adaptées) et de résilience des infrastructures numériques (plans de continuité et de reprise d'activité). Des clauses spécifiques de confidentialité devront être intégrées aux contrats de sous-traitance éventuels et des procédures de gestion des incidents de sécurité devront être opérationnelles dès le début du marché.

5.5 Amélioration continue

Au-delà du maintien en conditions opérationnelles, le titulaire devra s'inscrire dans une logique d'amélioration continue des prestations. Il est attendu qu'il formule des propositions régulières d'évolution technique (montée de version, rationalisation d'architecture, sécurité), organisationnelle (refonte des processus, automatisation, amélioration des circuits de support) ou contractuelle (ajustement des SLA, périmètres de prestation), en lien avec les enjeux de maîtrise budgétaire, d'efficience organisationnelle et de qualité de service.

Ces propositions devront être documentées, argumentées et intégrées aux instances de suivi du marché pour évaluation, validation ou planification.

5.6 Documentation, supervision et outils

Le titulaire devra mettre en œuvre et maintenir une base de données de gestion de configuration (CMDB) exhaustive, permettant une visualisation et un suivi rigoureux des composantes techniques du système d'information. Cette CMDB devra intégrer l'ensemble des équipements, logiciels, interconnexions et services numériques déployés au sein de la collectivité. Elle devra être structurée selon des référentiels reconnus (ITIL, ISO/IEC 20000) et faire l'objet de mises à jour régulières, notamment à l'occasion des opérations de maintenance, de renouvellement, ou d'intégration de nouveaux périmètres.

Dans le cadre du pilotage opérationnel, le titulaire produira des rapports mensuels détaillés. Ces rapports comprendront des indicateurs de performance (SLA), des éléments de volumétrie, une analyse des incidents, des alertes de sécurité, ainsi qu'une synthèse des actions correctives ou préventives mises en œuvre. Des rapports spécifiques seront également attendus en fonction des tranches conditionnelles activées, permettant un suivi différencié et documenté des volets techniques et fonctionnels concernés.

Enfin, des tableaux de bord dynamiques et partagés devront être mis à disposition de la collectivité. Ces outils devront permettre une consultation en temps réel des principaux

indicateurs de service, accessibles aux responsables désignés de la commune et contribuer à renforcer la transparence, la gouvernance et l'anticipation des décisions relatives au système d'information.

6 Réversibilité

6.1 Objet, principes et calendrier

La réversibilité a pour objet de garantir, à tout moment, la reprise maîtrisée des services par la ville, un nouveau titulaire ou en réinternalisation, sans interruption non planifiée ni perte de données. Dès le démarrage du marché (T0), le titulaire élabore un plan de réversibilité détaillé, validé par la DSI, précisant le calendrier, les jalons, les responsabilités (RACI), les livrables, les environnements concernés et les conditions de bascule. Ce plan est mis à jour au fil du marché et activé à l'issue du contrat, en cas de résiliation ou sur décision de la ville, dans les délais et modalités précisés au CCAP.

6.2 Périmètre des éléments à transférer

Le titulaire remet l'ensemble des éléments nécessaires à la continuité du service, notamment :

- Données et contenus : sauvegardes vérifiées, jeux de données, historiques nécessaires à l'exploitation et au support ;
- Comptes, identités et habilitations : inventaire des comptes (techniques et nominaux), matrices d'habilitation, politiques d'accès (MFA, accès conditionnel), procédures de création/suppression ;
- Paramétrages et configurations : Active Directory, DNS/DHCP, groupes, GPO, politiques de sécurité, règles pare-feu, configurations réseau (VLAN, routage, Wi-Fi, VPN, bastion), VDI Citrix, sauvegardes, supervision ;
- Environnements Microsoft 365 : structure du tenant, domaines, licences, groupes, SharePoint/OneDrive/Teams, politiques de sécurité et conformité ;
- Outils ITSM : GLPI (incidents, demandes, inventaire, CMDB, base de connaissance, rapports) ;
- Secrets et certificats : inventaire des certificats (Certinomis et autres), clés privées et matériels associés, coffre-fort de secrets, dates d'échéance, procédures de renouvellement ;
- Scripts et outillage : scripts d'exploitation et de déploiement, modèles GPO, modèles de configuration, playbooks/runbooks (PRA/PCA, sauvegardes, mises à jour) ;
- Documentation : dossiers d'architecture, cartographies L2/L3, plan d'adressage, matrice de flux, procédures d'exploitation, dossiers d'exploitation site, trames de rapports ;
- Interfaces et intégrations : contrats d'API, spécifications ETL, paramètres d'interconnexion (locaux/SaaS), dossiers de tests, jeux de données de recette ;
- Journalisation : journaux des accès d'administration et de sécurité (conservation minimale 12 mois) exportés dans un format exploitable.

Tous les fichiers et exports sont remis dans des formats ouverts et interopérables (CSV, JSON, XML, YAML, OpenAPI, PDF/A pour la documentation).

6.3 Livrables obligatoires

- Plan de réversibilité T0 (et mises à jour annuelles) ;
- Inventaires complets : CMDB exportée, parc matériel, licences et contrats, certificats, comptes et habilitations ;
- Dossiers d'exploitation par domaine (réseau, système, VDI, sauvegardes, Wi-Fi, M365, GLPI) ;
- Catalogue des interfaces (API/ETL) avec contrats, schémas et procédures ;
- Coffre-fort de secrets remis à la ville selon une procédure sécurisée (double contrôle) ;
- Jeux de sauvegardes et procès-verbaux de restauration témoin ;
- Procès-verbaux de transfert (accès, droits, matériels, documentations).

6.4 Transfert de compétences et accompagnement

Le titulaire organise un transfert de compétences au profit de la DSI et/ou du futur exploitant :

- Sessions de formation ciblées (exploitation courante, sécurité, MS365, GLPI, supervision) ;
- Ateliers de passage de relais par périmètre avec démonstrations et Q/R ;
- Remise des supports pédagogiques, procédures et check-lists ;
- Accompagnement à la prise en main pendant la période de transition.

6.5 Modalités de co-exploitation et bascule

La réversibilité peut inclure une période de co-exploitation convenue (double commande limitée) pour sécuriser la bascule. Durant cette période :

- Gel partiel des changements non essentiels ;
- Accès conjoints et tracés sur les consoles d'administration ;
- Plan de communication et points quotidiens de suivi ;
- Bascule progressive par lots (réseau, sauvegardes, VDI, M365, sites), avec procès-verbaux de recette à chaque étape.

Le titulaire coordonne les interfaces avec les prestataires tiers (Ineo pour les liaisons, SFR Business pour la téléphonie, Kyocera pour l'impression, exploitant du CSU pour les dépendances réseau), afin d'éviter toute rupture de service.

6.6 Critères de recette de la réversibilité

La réversibilité est réputée conforme lorsque, au minimum :

- Accès d'administration remis à la ville/nouveau titulaire (comptes, MFA, bastion) et retrait des accès du titulaire sortant ;
- CMDB et inventaires remis, complets et concordants (taux de complétude ≥ 98 % sur les attributs obligatoires) ;
- Restauration témoin d'un serveur critique et d'un poste type réalisée avec succès ;
- Supervision opérationnelle chez le repreneur (sondes, seuils, tableaux de bord actifs) ;
- Interfaces critiques testées en bout-en-bout, sans régression ;
- Documentation remise et validée (architecture, procédures, runbooks, contrats d'interface) ;
- Journalisation exportée et vérifiée (période minimale 12 mois) ;
- Procès-verbaux de transfert signés par les parties.

Tout écart majeur fait l'objet d'un plan d'actions correctif sous délais. Les pénalités associées sont précisées au CCAP

6.7 Protection des données et conformité

Le titulaire applique les obligations du RGPD en qualité de sous-traitant : remise/retour des données à caractère personnel, effacement sécurisé des copies après transfert (avec attestation), mise à jour du registre des traitements impactés, information du DPO. Les mesures de sécurité demeurent en vigueur jusqu'à la clôture effective de la réversibilité.

6.8 Clauses de loyauté et responsabilités

Le titulaire s'engage à une assistance loyale et neutre pendant la transition, sans facturation redondante ni rétention d'information. Il s'interdit toute dépendance technique empêchant la portabilité. Les conditions financières de la réversibilité (forfait inclus, unités complémentaires le cas échéant) et les pénalités en cas de manquement relèvent du CCAP et du BPU/DQE.

7 Clauses spécifiques

7.1 Propriété intellectuelle, technique et documentaire

La Ville demeure seule propriétaire de l'ensemble des actifs informationnels et techniques liés au service public numérique : données, contenus, configurations et paramétrages, comptes et identifiants (y compris tenants Microsoft 365, noms de domaine, certificats et clés), scripts et outillages, modèles (GPO, masters, images VDI), documentation (dossiers d'architecture, procédures, runbooks), contrats d'interface (API/ETL) et rapports.

Le titulaire cède à la Ville, à titre exclusif et sans limitation de durée ni de territoire, les droits patrimoniaux attachés aux livrables créés dans le cadre du marché, à l'exception des éléments préexistants dont il demeure titulaire (auquel cas une licence d'utilisation non exclusive, non transférable et gratuite est concédée pour les besoins d'exploitation, de maintenance et de réversibilité).

Tous les livrables sont remis à première demande en formats ouverts et interopérables (par exemple : CSV, JSON, XML, YAML, OpenAPI, PDF/A) et intégrés à la CMDB et au référentiel documentaire de la collectivité.

7.2 Absence de dépendance technique et neutralité du titulaire

Le titulaire s'interdit toute mise en œuvre de mécanismes de verrouillage technologique (verrou propriétaire, dépendance non documentée, accès exclusif) empêchant ou renchérissant la maintenance par un tiers ou la réversibilité.

Toute solution ou composant non expressément prévu au marché et susceptible de créer une dépendance (module propriétaire, service managé imposant un compte éditeur contrôlé par le titulaire, bastion ou supervision opérés hors du contrôle de la Ville) doit faire l'objet d'une validation préalable de la DSI, avec démonstration de la réversibilité (export complet des données, portage des configurations, transfert des droits d'accès).

Les accès d'administration sont nominatifs, soumis à MFA, tracés et les comptes « super administrateur » ne peuvent être détenus exclusivement par le titulaire. Les secrets et clés sont gérés dans un coffre-fort accessible à la Ville.

7.3 Portabilité, interopérabilité et accessibilité

Le titulaire garantit la portabilité des données et des configurations pendant toute la durée du marché et à son terme : export complet, cohérent et vérifiable, accompagné des schémas, dictionnaires et contrats d'interface.

L'interopérabilité est assurée par la priorité aux standards ouverts (API REST/JSON documentées – OpenAPI, SSO SAML/OIDC, SFTP/AS2 pour les flux réglementaires, schémas de données partagés), une politique de versionnage et de dépréciation et la disponibilité d'un catalogue d'interfaces à jour.

L'accessibilité numérique des services et portails mis en œuvre est conforme au RGAA en vigueur ; le titulaire fournit une déclaration d'accessibilité, un plan d'actions en cas d'écarts et se soumet, à la demande, à des audits d'accessibilité.

7.4 Journalisation, auditabilité et transparence

Les accès d'administration, événements de sécurité et opérations sensibles font l'objet d'une journalisation horodatée, inaltérable et conservée au minimum 12 mois. Les journaux sont accessibles à la Ville et exportables en formats ouverts.

La Ville se réserve un droit d'audit (technique, sécurité, RGPD, accessibilité) directement ou par un tiers mandaté ; le titulaire coopère pleinement, met à disposition les environnements, preuves et personnels et met en œuvre sans délai les plans d'actions correctifs validés par la DSI.

7.5 Protection des données (RGPD) et sous-traitance

Le titulaire agit en qualité de sous-traitant au sens du RGPD. Une convention de traitement (DPA) précise les finalités, catégories de données, mesures de sécurité, modalités d'exercice des droits et d'assistance au DPO.

Toute violation de données ou incident de sécurité susceptible d'affecter la confidentialité, l'intégrité ou la disponibilité des traitements est notifié sans délai injustifié à la Ville, avec information circonstanciée et mesures conservatoires.

Toute sous-traitance en chaîne (sous-traitant de second rang) est soumise à autorisation préalable de la Ville ; les obligations du présent marché sont intégralement répercutées par le titulaire à ses sous-traitants.

7.6 Réutilisation, confidentialité et propriété des comptes

Les livrables, configurations et documents produits ne peuvent être réutilisés par le titulaire à d'autres fins sans accord écrit de la Ville. Des clauses de confidentialité s'appliquent à l'ensemble des personnels et sous-traitants du titulaire.

Les comptes, tenants, noms de domaine et souscriptions (notamment Microsoft 365, certificats, hébergements et abonnements cloud) sont créés et détenus au nom de la Ville ; le titulaire n'utilise pas ses propres environnements ou identifiants éditeurs pour opérer les actifs de la collectivité, sauf dérogation expressément validée et réversible.

8 Modalités financières et d'exécution

8.1 Forme du marché et durée

Le marché est composite à prix mixtes :

- Une partie forfaitaire par tranches pour les prestations dont la consistance est précisément définie ;
- Une partie à bons de commande (accord-cadre mono-attributaire) pour les besoins ponctuels, l'intégration de nouveaux sites et les prestations complémentaires, exécutée au fur et à mesure de l'émission des bons conformément aux articles R.2162-13 et suivants.

La coexistence, au sein d'un même contrat, d'une partie « ordinaire » et d'une partie exécutée par bons de commande est admise dès lors que les catégories de prestations sont clairement distinguées.

La durée d'exécution globale du marché (forfait + accord-cadre) est fixée dans les pièces contractuelles. La partie accord-cadre comporte une durée et un maximum (annuel et/ou total), conformément aux règles applicables aux accords-cadres. Les tranches conditionnelles relèvent du régime des articles R.2113-4 à R.2113-6 (affermissement par décision de la ville, dans les délais et conditions prévus au marché).

8.2 Prix et structure de rémunération

- Partie forfaitaire (tranches) : prix forfaitaires couvrant l'intégralité des prestations prévues à chaque tranche (contenu, livrables, SLA et pénalités associées).
- Partie à bons de commande : prix unitaires issus d'un bordereau des prix unitaires (BPU) ; un DQE sert à l'analyse des offres. Chaque bon précise la quantité commandée et le prix correspondant. Les prestations éligibles à bons de commande sont listées et plafonnées (ex. intégration d'un nouveau site, renforts d'expertise, déploiement supplémentaire de clients légers, extensions Wi-Fi).
  Les composantes liées à des bons de commande évaluées à périmètre constant d'équipements et de serveurs à la date de formulation de l'offre ne devront pas dépasser 33 333,33 € HT soit 40 000€ TTC.

Les prix peuvent être fermes ou révisables selon la nature des prestations, conformément aux articles R.2112-5 à R.2112-18. Pour la partie révisable, la formule d'indexation est précisée au CCAP (exemple : part services indexée sur Index Syntec ou indice INSEE pertinent, part énergie/locaux techniques le cas échéant), avec périodicité, dates de référence, clause de sauvegarde et modalités en cas de disparition d'indice.

8.2.1 Plafond d’acceptabilité budgétaire

Le montant annuel TTC de la partie forfaitaire proposée par le candidat, hors prestations à bons de commande (BPU) et hors tranches conditionnelles non affermies, ne doit pas excéder 270000 € TTC/an.

Toute offre dont le montant excède ce plafond sera déclarée inacceptable et éliminée conformément aux articles L2152-1 et L2152-3 et selon la procédure, R2152-1 du code de la commande publique.

Le plafond est apprécié pour une année civile pleine ; en cas de première/dernière année incomplète, l’appréciation est faite au *prorata temporis*.

Ce plafond ne vaut pas minimum d’engagement et ne s’applique pas à la part exécutée par bons de commande.

8.3 Forfaits par tranches et jalons de facturation

- Tranche ferme 1 – Refonte et sécurisation : facturation par jalons (audit, dossier d’architecture cible, plan de transformation, PV de mise en conformité, PV de déploiement clients légers par lot).
- Tranche ferme 2 – Exploitation : facturation mensuelle au prorata de la période, conditionnée au service fait et à la remise du rapport mensuel SLA.
- Tranche ferme 3 – Support et coordination applicative : facturation mensuelle, assortie d’indicateurs GLPI (volumétrie, délais, satisfaction).

Les tranches conditionnelles sont rémunérées selon jalons (cartographie et catalogue d’interfaces ; diagnostic et plan d’actions sobriété).

8.4 Partie à bons de commande (accord-cadre)

La partie accord-cadre précise :

- Les prestations éligibles, les unités d’œuvre et les conditions d’intervention ;
- Le ou les plafonds (annuels et/ou sur la durée) exprimés en euros HT, assurant la prévisibilité budgétaire ;
- L’absence de minimum ou, le cas échéant, un minimum raisonnable ;
- La procédure d’émission des bons (objet, quantité, site, délais, pénalités applicables, circuits de visa) et leur rattachement à l’exercice budgétaire ;
- Les délais d’exécution par catégorie et les pénalités de retard.

Cette partie est exécutée par bons de commande au sens des articles R.2162-13 et suivants.

Précisions spécifiques au périmètre IaaS et DasS :

Un décommissionnement ou extinction de serveur devenu superflu selon l'appréciation validée par le client, sur demande exprès de la DSI et de la direction des ressources se traduira par une moins-value en termes de facturation. En d'autres termes, le bordereau de prix présenté par le prestataire prévoira ce cas de figure d'extinction de serveur ou d'autres équipements pivots de l'infrastructure informatique, dans la mesure où ce facteur réduira le temps de travail consacré au maintien en conditions opérationnelles et à la veille informatique de tels équipements neutralisés.

8.5 Règles budgétaires : annualité, prévisibilité, engagement des crédits

La ville organise l'exécution dans le respect du principe d'annualité :

- La partie forfaitaire est engagée par exercice, avec planification des jalons ;
- La partie à bons de commande est cadrée par des plafonds annuels, permettant d'anticiper l'engagement des crédits ;
- Les prestations commandées en fin d'exercice sont planifiées de façon à respecter le service fait et, le cas échéant, les règles comptables applicables (restes à réaliser).

Les reconductions éventuelles sont expresses et prévues au marché (pas de tacite reconduction).

8.6 Avances, acomptes et paiement

Avance : lorsque le montant initial du marché excède 50 000 € HT et que le délai d'exécution dépasse 2 mois, la ville verse une avance obligatoire au titulaire ; son taux est compris entre 5 % et 30 %, modulé selon la durée du marché (ou de la tranche) et les cas PME (taux minimum relevé dans certaines situations prévues par le code). Les modalités de calcul, de versement et de remboursement (y compris garanties éventuelles) sont précisées au CCAP.

Acomptes : des acomptes peuvent être versés au fur et à mesure du service fait (mensualités d'exploitation, PV de jalon).

Délai global de paiement (DGP) : 30 jours pour la collectivité ; au-delà, intérêts moratoires et indemnité forfaitaire de recouvrement sont dus de plein droit.

8.7 Pénalités de service et bonus qualité

Le CCAP fixe un barème de pénalités proportionné (retard, indisponibilités, non-respect des SLA, défauts documentaires, absence d'astreinte), avec un plafond par période (par exemple un pourcentage du montant annuel de la partie forfaitaire) afin de respecter le principe de proportionnalité.

La ville peut prévoir un mécanisme incitatif (bonus-malus) adossé à quelques indicateurs clés (ex. disponibilité cible dépassée, réduction mesurée du volume d'incidents, gains de sobriété au-delà de l'objectif), dans la limite d'un plafond annuel.

8.8 Décomposition des prix et transparence

Le titulaire remet, à l'offre et à première demande, une décomposition du prix global et forfaitaire (DPGF) par tranche et par lot technique, détaillant la part main-d'œuvre/logiciels/équipements, pour permettre les avenants éventuels en cas d'évolution de périmètre. Le BPU précise les unités d'œuvre, hypothèses d'intervention et franchissements de seuil (astreintes, heures non ouvrées).

8.9 Coordination budgétaire et pilotage administratif

Sous l'autorité de la DSI, la secrétaire dédiée et le technicien terrain :

- Suivent les engagements (forfaits, bons de commande, avances, acomptes) et alimente un tableau de suivi partagé ;
- Vérifient la concordance entre factures, bons de commande, PV de jalon et rapports SLA ;
- Préparent les certifications de service fait et veille au respect du DGP ;
- Alertent sur l'atteinte des plafonds annuels de la partie accord-cadre ;
- Tiennent à jour la traçabilité financière en lien avec la CMDB pour assurer la réversibilité.

8.10 Sous-traitance et cession de créances

La sous-traitance est autorisée dans les conditions du code ; les sous-traitants acceptés et agréés peuvent bénéficier du paiement direct. La cession ou le nantissement de créances est possible selon les modalités prévues par la réglementation ; les références des cessions sont portées sur les factures.

8.11 Articulation avec les autres marchés de la ville

Les fournitures et services déjà couverts par d'autres marchés (ex. Inmac W Store pour le matériel, SIPPEREC/SFR Business pour la téléphonie, Kyocera pour les copieurs, Ineo pour les liaisons fibre) ne sont pas rachetés dans le présent marché.

Le titulaire coordonne ses interventions avec ces titulaires, sans doublon de facturation ; les prestations d'intégration, de paramétrage ou de MCO relevant du SI communal sont rémunérées au forfait ou au BPU selon le périmètre.