EUROMĒDITERRANĒE
Établissement Public d'Aménagement - Marseille

Cahier des Clauses Techniques Particulières (CCTP)

INFRASTRUCTURE INFORMATIQUE ET SERVICES ASSOCIÉS

1. PREAMBULE

Le présent Cahier des Clauses Techniques Particulières définit les exigences techniques relatives au marché d'infrastructure informatique et services associés de l'Établissement Public d'Aménagement Euroméditerranée. Il a pour objet de préciser le périmètre des fournitures, prestations d'installation, prestations de migration, services de maintenance, supervision, cybersécurité, sauvegarde et accompagnement attendus du titulaire.

Le marché s'inscrit dans la continuité du précédent marché d'infrastructure, arrivé à échéance, tout en tenant compte de l'évolution des usages, de l'augmentation des risques cyber, de l'évolution des contraintes budgétaires et des objectifs de sobriété numérique. L'objectif recherché n'est pas le renouvellement systématique de tous les équipements, mais la mise en place d'une infrastructure fiable, sécurisée, pérenne et économiquement soutenable.

Le titulaire devra proposer une solution complète, cohérente et exploitable, permettant à l'établissement de maintenir la continuité de service de son système d'information, d'améliorer le niveau de sécurité global et de disposer d'une architecture administrable et documentée.

Dans le présent document, le terme remarketed (ou remarketé) désigne des équipements d'entreprise (serveurs, stockage, réseau) retournés au constructeur ou à un partenaire certifié, remis à neuf selon les standards d'usine et revendus avec une garantie constructeur complète.

2. CONTEXTE ET ARCHITECTURE EXISTANTE

2.1. DESCRIPTIF DE L'ARCHITECTURE TECHNIQUE EXISTANTE

L'établissement dispose actuellement d'une infrastructure informatique structurée autour d'un site principal situé dans ses locaux, d'un espace de Plan de Reprise d'Activité (PRA) situé au rez-de-chaussée et d'un dispositif de sauvegarde externalisée hébergé en datacenter.

L'infrastructure existante comprend notamment des hyperviseurs, une baie de stockage SAN, des équipements NAS, des pares-feux, un cœur de réseau, des commutateurs de distribution, des bornes Wi-Fi, des onduleurs, une solution de sauvegarde, une solution antispam, une solution de protection des postes et serveurs ainsi qu'un dispositif de supervision.

Le marché actuel 2021–2026 arrivant à son terme, l'établissement souhaite renouveler ou prolonger les composants nécessaires au maintien en condition opérationnelle de son système d'information. La démarche retenue consiste à privilégier, lorsque cela est techniquement pertinent, la réutilisation de l'existant, le recours à du matériel issu de filières de réemploi professionnel ou d'échange standard, ainsi que la prolongation de la durée de vie des équipements encore compatibles avec les besoins de production.

Le contexte de cybersécurité a également fortement évolué. Les attaques par rançongiciel, la compromission des identités, les mouvements latéraux dans les réseaux internes, l'exploitation de vulnérabilités et les attaques automatisées imposent désormais une approche de sécurité multicouche, centralisée et supervisée. Le marché intègre donc une solution de cybersécurité avancée couvrant les postes, les serveurs, les accès distants et, autant que possible, les événements réseau.

L’architecture existante est répartie entre plusieurs emplacements. Le site principal situé au R+1 de L’Astrolabe héberge les principales baies informatiques, les équipements de production, les équipements réseau, les éléments de sauvegarde chaude et le brassage. Le rez-de-chaussée héberge un espace dédié au Plan de Reprise d’Activité. Un datacenter externe héberge un équipement de sauvegarde immutable.

Emplacement	Éléments principaux	Usage
R+1 Astrolabe	3 Baies informatiques, 2 hyperviseurs, 1 SAN, 1 NAS, pares-feux redondé, cœur de réseau (L3), 5 switchs (L2), Wi-Fi (contrôleur + 15 bornes), 3 onduleurs	Production, réseau, sauvegarde chaude et administration
RDC Astrolabe	Baie PRA, hyperviseur/PRA et stockage associé, 1 switch et 1 onduleur	Plan de Reprise d’Activité local
Datacenter	Équipement NAS ou équivalent dédié à la sauvegarde immutable	Protection externalisée contre sinistres et compromissions

Périmètre dimensionnant

À titre indicatif, le périmètre actuel de l'établissement est le suivant.
Ces données sont fournies pour permettre le dimensionnement des licences et des prestations associées.

L'établissement compte environ 80 utilisateurs actifs et 85 postes de travail (fixes et portables).
Le parc serveur comprend 15 machines virtuelles en production sous OS mixte Windows, Linux.
L'accès distant doit couvrir 80 connexions VPN simultanées.
La capacité de stockage en production est d'environ 12 To utiles et la capacité de sauvegarde chaude et immutable d'environ 25 To utiles chacune.
Le PRA est dimensionné comme la production : 12To.

Ces volumes sont susceptibles d'évoluer modérément pendant la durée du marché. La solution devra être dimensionnée pour absorber une croissance raisonnable sans remise en cause de l'architecture.

2.2. INFRASTRUCTURE DE PRODUCTION

Architecture physique

L’infrastructure de production repose sur deux hyperviseurs en cluster et un stockage partagé de type SAN. Cette architecture permet l’hébergement des machines virtuelles nécessaires au fonctionnement des services internes. Le dispositif est complété par un PRA, des NAS de sauvegarde, des pares-feux, des équipements de commutation, des bornes Wi-Fi et des onduleurs.

Domaine	Équipements existants ou périmètre	Commentaires
Virtualisation	Deux hyperviseurs en cluster	Socle de production hébergeant les machines virtuelles
Stockage	SAN d'environ 12 To utiles	Stockage principal des données et machines virtuelles
PRA	Hyperviseurs + VSAN	Socle de plan de reprise d'activité
Sauvegarde	NAS internes et sauvegarde immutable externalisée 25To chacune	Sauvegarde chaude interne et sauvegarde protégée externe
Réseau	Pares-feux redondés, cœur de réseau niveau 3, switchs niveau 2	Routage, segmentation, distribution LAN et sécurité périmétrique
Wi-Fi	Bornes au R+1 et au RDC, contrôleur dédié	Réseaux Wi-Fi interne et invité
Énergie	Onduleurs associés aux équipements critiques	Protection électrique et arrêt propre

Machines virtuelles

Le parc serveur est composé d'un ensemble de machines virtuelles sous OS mixte, Windows et Linux, assurant les fonctions d'annuaire, fichiers, impressions, sauvegarde, applications métiers, bases de données, supervision, téléphonie, services techniques et services historiques.
Le titulaire devra établir, lors de la phase de cadrage, un inventaire actualisé des machines virtuelles, de leurs ressources, de leurs dépendances, de leurs systèmes d'exploitation et de leurs contraintes de disponibilité.
La solution proposée devra permettre de faire évoluer le nombre de machines virtuelles et leur volumétrie pendant la durée du marché. Elle devra également permettre la création de machines virtuelles supplémentaires pour les besoins de tests, de recettes, de migrations ou de nouveaux services.

Sauvegarde

La sauvegarde constitue un élément essentiel du présent marché. Le dispositif actuel s'appuie sur une solution de sauvegarde et de réplication permettant l'exécution de plusieurs jobs distincts : sauvegarde, réplication, sauvegarde renforcée et sauvegarde immutable. La solution cible devra reprendre ce principe, l'améliorer et garantir des capacités de restauration rapides, fiables et testées.

Plan de Reprise d'Activité

Le Plan de Reprise d'Activité doit permettre la reprise des services essentiels en cas de défaillance majeure de l'infrastructure de production. Le titulaire devra maintenir, optimiser et documenter le PRA existant. Il devra proposer une procédure de bascule, une procédure de retour arrière, un calendrier de tests et des engagements de temps de reprise adaptés aux moyens mis en œuvre.

2.3. RESEAU ET ACCES

Réseaux logiques

Le réseau de l'établissement est segmenté en plusieurs sous-réseaux ou VLAN afin de dissocier les usages et d'améliorer la sécurité. La solution proposée devra reprendre, documenter, optimiser et sécuriser cette segmentation en coordination avec le service informatique.

- Réseau principal destiné aux postes, serveurs, copieurs et équipements internes ;
- Réseau Wi-Fi interne ;
- Réseau dédié à la téléphonie sur IP ;
- Réseau Wi-Fi public ou invité, isolé du réseau interne ;
- Zone démilitarisée destinée aux services exposés ou segmentés.

Wi-Fi

Le réseau Wi-Fi couvre l'ensemble des zones nécessaires du R+1 et du RDC. Il comporte un réseau interne et un réseau public ou invité. Le réseau invité devra rester strictement isolé du réseau interne. La solution repose sur la conservation, la maintenance et, si nécessaire, la modernisation partielle du dispositif Wi-Fi existant.

VPN

Le VPN permet aux utilisateurs d'accéder à certaines ressources internes. Il est basé sur une connexion AD.
Il est basé sur des règles de sécurité liées aux pares-feux comme des règles de limitation géographiques.

2.4. SECURITE

Protection des postes et serveurs

La protection des postes utilisateurs et serveurs est actuellement assurée par une solution unifiée.
La protection est un point majeur de ce marché et la solution proposée devra être moderne et centralisée couvrant l'ensemble du périmètre. La solution ne devra pas se limiter à une fonction antivirus traditionnelle, mais intégrer des fonctions de détection comportementale, de réponse à incident et de supervision avancée.

Antispam

La solution antispam est actuellement externalisée et sans lien avec le Tenant MS365 de l'établissement. Elle permet de protéger l'établissement contre les menaces connues et de filtrer rapidement les messages entrant en se basant sur un score configuré par l'établissement.
La gestion des listes blanches / noirs se fait globalement et par utilisateur.
La quarantaine se fait par utilisateur, un rôle d'administrateur est accordé à l'établissement.

2.5. SERVICE D'ANNUAIRE ET DE MESSAGERIE

L'annuaire interne fonctionne en mode hybride avec les services Microsoft 365. Le titulaire devra prendre en compte cette organisation et accompagner l'établissement dans la gestion des comptes, groupes, stratégies, synchronisations, accès, droits et règles de sécurité associées. Les interventions devront être réalisées sans rupture de service et en coordination avec le service informatique.

2.6. MATERIELS HORS PERIMETRE OU A PRENDRE EN COMPTE

Certains équipements ou services peuvent être maintenus hors du périmètre direct du marché tout en ayant des interactions avec l'infrastructure.
Le titulaire devra les identifier lors de la phase de cadrage afin d'éviter toute interruption ou incompatibilité.
Il s'agit notamment des équipements liés à l'accès fibre, des équipements historiques, des périphériques d'impression connectés et des services applicatifs opérés par des prestataires tiers.

3. OBJECTIFS ET ARCHITECTURE CIBLE

L'objectif principal du marché est de mettre à disposition de l'établissement une infrastructure fiable, sécurisée, supervisée, maintenable et évolutive pour les cinq prochaines années. La solution devra garantir la continuité de service, la protection des données, la capacité de restauration, la maîtrise budgétaire et la réduction de l'impact environnemental.

Les services complémentaires de sauvegarde, VPN, licences CAL, supervision, antispam et licences serveur sont comprises dans le marché.

3.1. OPTIMISATION, REEMPLOI ET MAINTIEN DE L'EXISTANT

La solution de base est la réponse attendue prioritairement. Elle repose sur la conservation des équipements existants lorsque ceux-ci restent compatibles avec les exigences techniques, sur le remplacement ciblé des composants réellement nécessaires et sur le recours à des équipements issus de filières professionnelles de réemploi, d'échange standard ou de matériel remarketed lorsque cela est pertinent.

- Utiliser du matériel remarketed ou équivalent pour les hyperviseurs, les équipements de stockage et les NAS lorsque le niveau de garantie et de support est satisfaisant ;
- Conserver et maintenir le dispositif Wi-Fi existant, en prévoyant une modernisation partielle uniquement si nécessaire ;
- Remplacer prioritairement les batteries des onduleurs, avec un bordereau de prix unitaire permettant leur remplacement complet en cas de défaillance ;
- Conserver les switchs de niveau 2 lorsque leur état, leur support et leur capacité de supervision sont compatibles avec les exigences du marché ;
- Renforcer la cybersécurité, la sauvegarde, la supervision et la documentation, indépendamment de la logique de réemploi retenue.

3.2. ARCHITECTURE CIBLE ATTENDUE

L'architecture cible devra permettre l'hébergement des services actuels et futurs, la haute disponibilité des services critiques, la sauvegarde régulière des données, la réplication vers le PRA, l'administration centralisée, la supervision proactive et la protection avancée contre les menaces.
Elle devra rester exploitable par le service informatique de l'établissement au quotidien.

Composant	Exigence
Hyperviseurs dont PRA	Échange standard, reconditionné professionnel ou remplacement ciblé et garanti.
Stockage SAN	Maintien ou remplacement remarketed compatible et garanti.
NAS sauvegarde	Maintien, extension ou équipement reconditionné et garanti.
Wi-Fi	Conservation et maintenance du dispositif actuel, modernisation partielle possible.
Onduleurs	Remplacement des batteries et tests.
Switchs N2	Conservation, mise à jour et supervision.
Switch N3 – cœur de reseau	Remplacement avec matériel équivalent.
Pares-feux	Remplacement Matériel redondé, interface d'administration onPremise.
Cybersécurité	Solution avancée obligatoire

3.3. EXIGENCES RENFORCEES EN CYBERSECURITE

La cybersécurité constitue un axe structurant du présent marché. Le titulaire devra proposer une solution unifiée et centralisée couvrant les postes utilisateurs, les serveurs physiques et virtuels, les accès distants et, autant que possible, les événements réseau. La solution devra intégrer des fonctions de protection, de détection, d'investigation, de réponse aux incidents et de reporting.
L'intégration de la solution couvrira la désinstallation de la solution actuellement utilisée.

Protection des postes et serveurs

La solution devra inclure une protection de type EPP, capable d'assurer la protection antivirus nouvelle génération, l'analyse en temps réel, la protection anti-ransomware, le contrôle des comportements suspects et la protection des charges serveurs. La gestion devra être centralisée et permettre le suivi de la conformité de l'ensemble du parc.

Détection avancée et corrélation

La solution devra intégrer des capacités de type EDR et XDR permettant d'identifier les activités anormales, les mouvements latéraux, les escalades de privilèges, les exécutions suspectes, les connexions inhabituelles et les comportements pouvant traduire une compromission. La corrélation des événements devra faciliter l'analyse des incidents et réduire le temps de réaction.

Réponse aux incidents

La solution devra permettre l'isolement d'un poste compromis, le blocage de processus malveillants, la mise en quarantaine de fichiers, la remédiation automatisée ou assistée, ainsi que la conservation des éléments nécessaires à l'investigation. Le titulaire devra décrire précisément les actions automatiques disponibles et les actions nécessitant une validation humaine.

Supervision managée

Le titulaire devra proposer un service de supervision et de traitement des alertes de sécurité. Ce service pourra prendre la forme d'une prestation MDR ou d'un dispositif équivalent de surveillance, qualification et accompagnement à la réponse aux incidents.

Le service de supervision des alertes de sécurité devra couvrir à minima les heures ouvrées (lundi au vendredi, 9h00-18h00 hors jours fériés). Le titulaire pourra proposer en option une extension de cette couverture en dehors des heures ouvrées (soirs, nuits, week-ends), dont le coût sera présenté distinctement dans l'annexe financière.

Pendant les heures couvertes, le titulaire devra assurer la qualification des alertes, leur priorisation, la notification au service informatique de l'établissement et, le cas échéant, la mise en œuvre des premières mesures de remédiation conformément aux procédures validées lors du cadrage.

Exigences d'administration

La solution devra disposer d'une console unique ou d'un portail centralisé accessible via navigateur, permettant la gestion des politiques, la consultation des alertes, le suivi de l'état des agents, la génération des rapports et l'administration des réponses à incident. La solution devra permettre une gestion simple des licences en cas d'arrivée ou de départ de collaborateurs.

Notification des incidents de sécurité

En cas d'incident de sécurité affectant l'infrastructure de l'établissement (compromission avérée ou suspectée, détection d'un comportement malveillant, exfiltration de données, déploiement d'un rançongiciel, exploitation d'une vulnérabilité), le titulaire pourra intervenir dans un cadre défini en amont et devra notifier l'établissement dans un délai maximal de quatre heures à compter de la détection de l'incident.

Cette notification devra indiquer la nature de l'incident, le périmètre potentiellement affecté, les premières mesures de confinement engagées et le plan d'action envisagé. Un rapport complet devra être transmis dans les 48 heures suivant la détection.

Le titulaire devra coopérer pleinement avec l'établissement et, le cas échéant, avec les autorités compétentes (ANSSI, CNIL) en cas d'investigation liée à un incident de sécurité.

3.4. SERVICES COMPLEMENTAIRES

Sauvegarde

Le titulaire devra proposer un plan de sauvegarde complet basé sur l'existant et comprenant des sauvegardes quotidiennes, hebdomadaires et mensuelles, une rétention adaptée aux besoins de l'établissement, une protection contre la suppression malveillante ou accidentelle, ainsi que des tests réguliers de restauration.

La solution de sauvegarde concerne les serveurs, elle doit être unifiée et permettre de gérer plusieurs jobs distincts à destination de différents emplacements (3-2-1) :

- Sauvegarde chaude, internalisée dans les locaux, permettant de récupérer facilement un serveur complet ou des fichiers unitaires. La sauvegarde chaude doit permettre de récupérer 7 jours glissants à minima.
- PRA : sauvegarde quotidienne de l'infrastructure de production sur emplacement dédié dans les locaux.
- Sauvegarde immutable : sauvegarde déportée offrant une copie de données qui ne peut **être ni modifiée, ni supprimée, ni chiffrée** pendant une période de rétention prédéfinie. Celle-ci devra couvrir à minima 4 mois de données à raison d'une sauvegarde mensuelle.

VPN

Les accès distants devront permettre aux utilisateurs autorisés d'accéder aux ressources internes de façon sécurisée. La solution cible devra privilégier un VPN IPsec ou une technologie équivalente présentant un niveau de sécurité robuste, une administration centralisée, une traçabilité des connexions et une intégration cohérente avec les règles de sécurité de l'établissement. La solution devra permettre une adaptation simple du nombre de licences en cas d'évolution des effectifs.

Antispam

La solution antispam devra protéger les flux de messagerie contre les courriers indésirables, les campagnes d'hameçonnage, les pièces jointes malveillantes et les liens frauduleux. Elle devra permettre l'administration centralisée des règles, la consultation des quarantaines, la génération de rapports et l'adaptation simple des licences en cas d'évolution du nombre de comptes.
L'intégration de l'antispam reprendra les boites emails actives au jour de l'intégration.

Licences CAL

Permettant de couvrir l'accès au réseau pour 80 collaborateurs.
Les licences supplémentaires devront être intégrée au BPU.

Licences Serveur

Le parc compte actuellement 8 serveurs Windows 2019, le titulaire devra proposer la migration vers des licences compatibles avec une durée de support équivalente ou supérieure à la durée du marché.

Les licences supplémentaires devront être intégrée au BPU.

4. PRESTATIONS DE DEPLOIEMENT

1.1 PHASE DE CADRAGE

Au démarrage du marché, le titulaire organisera une phase de cadrage avec le service informatique. Cette phase permettra de valider l'inventaire de l'existant, les contraintes de planning, les dépendances applicatives, les priorités de migration, les risques identifiés et les modalités de recette.

- Inventaire physique et logique de l'infrastructure ;
- Analyse de l'état des équipements conservés ;
- Validation de la stratégie de réemploi ;
- Planning détaillé de déploiement ;
- Plan de retour arrière et plan de continuité pendant migration.

1.2 INSTALLATION ET MISE EN ŒUVRE

Le titulaire assurera l'ensemble des prestations nécessaires à la mise en œuvre de la solution retenue. Il devra procéder à la sauvegarde de l'existant avant intervention, préparer les équipements, réaliser les installations physiques, effectuer les configurations réseau, intégrer les systèmes, migrer les données et valider le fonctionnement des services.

- Installation ou maintien des équipements serveurs, stockage, sauvegarde et réseau ;
- Reprise et optimisation du brassage lorsque nécessaire ;
- Configuration des VLAN, règles de routage, qos et règles de sécurité ;
- Migration ou adaptation des machines virtuelles ;
- Configuration des sauvegardes, réplications et tests de restauration ;
- Déploiement de la solution de cybersécurité ;
- Validation du Wi-Fi interne et invité ;
- Recette technique complète.

1.3 DELAIS DE DEPLOIEMENT

Le déploiement de la solution devra être achevé et la recette complète prononcée au plus tard le 31 décembre 2026, afin d'assurer la continuité de service avec le marché d'infrastructure en cours, qui prend fin à cette date.

Le délai global de déploiement de la solution, depuis la notification du marché jusqu'à la recette complète, ne devra pas excéder six semaines, sauf justification expresse validée par l'établissement. Ce délai inclut les phases de cadrage, commande ou mobilisation des matériels, préparation, installation, paramétrage, migration, tests, recette et transfert de compétences.

En cas de difficulté susceptible de compromettre le respect de cette échéance, le titulaire devra en informer l'établissement sans délai et proposer un plan de rattrapage. Tout dépassement du délai devra faire l'objet d'une justification expresse validée par l'établissement.

La continuité d'activité devra être garantie pendant toute la durée du déploiement.

1.4 TRANSPORT ET LIVRAISON

Les frais de transport, d'emballage, d'assurance et de manutention des matériels jusqu'au lieu de destination finale sont à la charge exclusive du titulaire.
La livraison s'effectuera sous la responsabilité du titulaire à l'adresse de l'établissement, notamment sur le site de L'Astrolabe, ainsi que, le cas échéant, sur le site de sauvegarde externalisée ou tout site indiqué par l'établissement pour les besoins du projet.
Le titulaire devra prévenir l'établissement suffisamment en amont de toute livraison ou intervention nécessitant un accès physique aux locaux techniques. Toute livraison non planifiée pourra être refusée.

5. PRESTATIONS DE MAINTIEN EN CONDITION OPERATIONNELLE

2.1 MAINTENANCE GLOBALE ET GARANTIE

La maintenance débute à compter de la recette de la solution. Elle couvre l'ensemble de l'architecture faisant l'objet du marché, qu'il s'agisse d'équipements conservés, reconditionnés, remplacés ou nouvellement fournis.
Le titulaire devra assurer le maintien en condition opérationnelle, l'assistance à l'administration, la supervision, le suivi des sauvegardes, les mises à jour et l'accompagnement en cas d'incident.

- Support téléphonique et courriel pendant les heures ouvrées ;
- Prise en compte rapide des incidents bloquants ;
- Interventions de télémaintenance sans limitation dans le cadre du MCO ;
- Interventions sur site lorsque la télémaintenance ne permet pas la résolution ;
- Suivi des garanties constructeur ou garanties équivalentes ;
- Rapport périodique de maintenance et recommandations d'amélioration.

Le support technique du titulaire devra être accessible du lundi au vendredi, de 9h00 à 13h00 et de 14h00 à 18h00, à l'exception des jours fériés légaux. Le support sera joignable par téléphone et par courriel.
Il est recommandé pour le titulaire de proposer une interface de suivi des demandes (helpdesk) permettant un suivi horodaté des incidents et des interventions.

Niveau d'incident	Description	Délai de prise en compte	Délai d'intervention sur site
Critique	Interruption majeure d'un service essentiel ou risque sécurité important	30 minutes maximum	4 heures ouvrées
Majeur	Dégradation significative d'un service ou impossibilité pour plusieurs utilisateurs	2 heures ouvrées	Journée ouvrée en cours ou suivante
Mineur	Incident ponctuel ou demande d'assistance sans impact majeur	4 heures ouvrées	Planifié d'un commun accord
Évolution	Demande d'amélioration, conseil ou modification non urgente	5 jours ouvrées	Planifié d'un commun accord

La prise en compte s'entend comme l'accusé de réception qualifié de l'incident, incluant un premier diagnostic et la communication d'un plan d'action au service informatique de l'établissement.

Les évolutions hors périmètre feront l'objet d'un devis et se dérouleront en mode projet.

2.2 EXTENSION DE GARANTIE CONSTRUCTEUR OU GARANTIE EQUIVALENTE

Les matériels fournis neufs devront bénéficier d'une garantie constructeur d'une durée minimale de cinq ans, sauf justification contraire acceptée par l'établissement. Les matériels issus de filières de réemploi ou d'échange standard devront bénéficier d'une garantie professionnelle équivalente, clairement décrite. Le titulaire assurera l'interface avec les constructeurs, distributeurs, éditeurs ou filières de garantie concernées.

2.3 SUPERVISION

Le titulaire devra mettre en place ou maintenir une supervision de l'infrastructure couvrant les équipements physiques, les machines virtuelles, les sauvegardes, les espaces disques, les services critiques, les équipements réseau, les onduleurs et les alertes de cybersécurité. Les alertes devront être qualifiées afin d'éviter une volumétrie excessive non exploitable.

Des rapports de supervision devront être transmis périodiquement à l'établissement. Ils devront présenter l'état général de l'infrastructure, les incidents constatés, les actions réalisées, les tendances de capacité et les recommandations.

Les rapports de supervision seront transmis mensuellement. Ils comprendront à minima : l'état de santé des équipements physiques et virtuels, le taux de disponibilité des services critiques, les incidents survenus et les actions correctives réalisées, l'état des sauvegardes et des tests de restauration, l'évolution de la consommation des ressources (CPU, mémoire, stockage) et les alertes de cybersécurité qualifiées.

Un comité de suivi technique se tiendra au moins une fois par trimestre entre le titulaire et le service informatique de l'établissement. Il permettra de faire le point sur l'état général de l'infrastructure, les incidents récurrents, les évolutions à prévoir et les recommandations du titulaire. Un compte rendu sera rédigé par le titulaire et transmis dans les cinq jours ouvrés suivant la réunion.

2.4 SAUVEGARDE ET PRA EN EXPLOITATION

Le titulaire devra assurer le suivi du plan de sauvegarde, sa documentation et son amélioration continue. Les tests de restauration devront être réalisés régulièrement.
Le PRA devra faire l'objet d'un test au moins semestriel, incluant un compte rendu, les difficultés rencontrées, les corrections proposées et les délais observés.

Cycles de rétention minimaux

Type de sauvegarde	Fréquence	Rétention minimale	Destination
Sauvegarde incrémentale (chaude)	Quotidienne	7 clichés glissants	NAS interne
Sauvegarde complète (chaude)	Hebdomadaire	4 clichés glissants	NAS interne
Sauvegarde complète PRA	Quotidienne	4 clichés glissants minimum	PRA
Sauvegarde immutable (froide)	Mensuelle	4 mois glissants minimum	Sauvegarde externalisée

Les sauvegardes hebdomadaires et mensuelles devront être des sauvegardes complètes.
La sauvegarde immutable devra intégrer un dispositif empêchant toute suppression ou altération des clichés, y compris par un compte disposant de privilèges d'administration. Le titulaire devra décrire précisément les mécanismes d'inaltérabilité mis en œuvre.

La capacité de la solution de sauvegarde devra être mise en adéquation avec la capacité du stockage de production et ne devra pas être inférieure à 25 To exploitables. Elle devra pouvoir être étendue par simple ajout de disques.

Les tests de restauration devront être réalisés régulièrement.

Objectifs de reprise PRA

Scénario de défaillance	Tems de reprise maximal (RTO)	Perte de données maximale (RPO)	Mode de bascule
Défaillance d'un hyperviseur	Moins d'une minute	Aucune perte	Automatique
Défaillance du stockage SAN principal	Moins d'une demi-journée	Un jour maximum	Manuel
Sinistre majeur affectant le site principal (incendie, inondation, compromission généralisée)	Moins de deux journées ouvrées	Une journée maximum si sauvegarde chaude ou PRA disponible. Un mois maximum si sauvegarde immutable uniquement disponible.	Manuel

Le titulaire devra dimensionner la sauvegarde et le PRA en cohérence avec ces objectifs.
Le PRA devra faire l'objet d'un test au moins semestriel, incluant un compte rendu, les difficultés rencontrées, les corrections proposées et les délais observés.
Ces tests devront vérifier la capacité effective à respecter les engagements de RTO et RPO définis ci-dessus.

2.5 MISE A JOUR DES LOGICIELS

Les logiciels, firmwares, agents, consoles et composants nécessaires au fonctionnement de l'architecture devront être maintenus à jour pendant toute la durée du marché.
Les mises à jour devront être qualifiées, planifiées et réalisées de manière à limiter les risques d'interruption. Les mises à jour de sécurité critiques devront faire l'objet d'un traitement prioritaire.

2.6 PRESTATIONS ET FOURNITURES COMPLEMENTAIRES

En complément des prestations forfaitaires décrites ci-dessus, des prestations d'ingénierie, des fournitures de matériel de remplacement ou d'extension et des licences supplémentaires pourront être commandées en cours de marché selon les besoins de l'établissement. Les tarifs applicables sont ceux du bordereau de prix unitaires. Les modalités de commande sont définies au CCAP.

6. OBLIGATIONS TRANSVERSALES

3.1 CONFIDENTIALITE

Le titulaire est soumis à une obligation stricte de confidentialité pour l'ensemble des informations, documents, identifiants, configurations, accès, schémas, règles de sécurité, données techniques ou organisationnelles dont il aurait connaissance dans le cadre du présent marché. Cette obligation s'applique à l'ensemble des personnels, sous-traitants et partenaires mobilisés par le titulaire.

Le titulaire s'interdit de communiquer à des tiers tout élément concernant l'architecture, les vulnérabilités, les accès, les données ou les dispositifs de sécurité de l'établissement, sauf accord écrit préalable de la personne publique ou obligation légale. Le titulaire devra mettre en œuvre les mesures internes nécessaires pour garantir la confidentialité des informations manipulées pendant toute la durée du marché et après son terme.

3.2 SPECIFICATIONS ENVIRONNEMENTALES GENERALES

Le présent marché s'inscrit dans une démarche de numérique responsable. Le titulaire devra justifier les choix techniques retenus au regard de la durabilité, de la réparabilité, de la consommation énergétique et de la limitation des déchets d'équipements électriques et électroniques.

La solution devra favoriser la réutilisation, l'échange standard, le matériel reconditionné professionnel ou remarketed, ainsi que le maintien des équipements existants lorsque ces derniers restent compatibles avec les exigences de sécurité, de performance, de supervision et de maintenance.

Les matériels réemployés devront bénéficier de garanties clairement définies, d'une traçabilité documentée et de conditions de remplacement en cas de défaillance.

Le titulaire devra en outre :

- Proposer des équipements économes en énergie et adaptés aux besoins réels de l'établissement ;
- Éviter le surdimensionnement injustifié ;
- Favoriser les équipements réparables, évolutifs et disposant d'un support documenté ;
- Prévoir la reprise, le recyclage ou la valorisation des équipements effectivement remplacés ;
- Documenter les gains attendus en matière de réduction de coût, de réduction de déchets et de prolongation du cycle de vie matériel.

3.3 TRANSFERT DE COMPETENCES

Le titulaire devra assurer un transfert de compétences vers le service informatique de l'établissement.
Ce transfert devra permettre l'administration courante de la solution, la consultation des consoles, le suivi des sauvegardes, la gestion des alertes, la manipulation des procédures de restauration, la compréhension de l'architecture et la capacité à dialoguer efficacement avec le support du titulaire.

- Administration de la virtualisation et des stockages ;
- Administration réseau et Wi-Fi ;

- Gestion de la sauvegarde et du PRA ;
- Exploitation de la solution de cybersécurité ;
- Administration de l'antispam ;
- Lecture des tableaux de bord et rapports de supervision ;
- Procédures d'incident, d'escalade et de retour arrière.

3.4 REVERSIBILITE (TRANCHE OPTIONNELLE)

À l'échéance du marché ou en cas de résiliation, le titulaire devra assurer le transfert complet et ordonné de l'ensemble des éléments nécessaires à la continuité d'exploitation de l'infrastructure par l'établissement ou par un tiers désigné.

La prestation de réversibilité comprendra notamment :

- La remise de l'intégralité des mots de passe, identifiants, certificats, clés de chiffrement et codes d'accès relatifs à l'infrastructure, aux équipements, aux consoles d'administration et aux services supervisés ;
- La remise de la documentation technique à jour, conforme aux exigences de l'article Documentation et dossier technique d'architecture du présent CCTP ;
- La remise des configurations sauvegardées des équipements réseau, pares-feux, switchs, contrôleur Wi-Fi et de tout équipement administrable ;
- La remise des données de supervision, historiques d'incidents et rapports produits pendant la durée du marché ;
- Le transfert des licences logicielles cessibles à l'établissement, ou à défaut l'information nécessaire pour que l'établissement puisse les renouveler directement auprès des éditeurs ;
- L'accompagnement du nouveau prestataire ou du service informatique pendant une période de transition d'une durée minimale de 8 semaines, incluant la présentation de l'architecture, les accès, les procédures d'exploitation et la réponse aux questions techniques.

Le titulaire ne pourra subordonner la remise de ces éléments au règlement d'un litige ou d'une facture en cours.

Les obligations de réversibilité s'appliqueront quelle que soit la cause de la fin du marché.

3.5 DOCUMENTATION ET DOSSIER TECHNIQUE D'ARCHITECTURE

À l'issue de la prestation de prise en main et avant la recette définitive, le titulaire remettra une documentation complète en langue française. Cette documentation devra être suffisamment précise pour permettre à l'établissement de comprendre, exploiter, maintenir et faire évoluer l'architecture.

- Schéma d'architecture physique ;
- Schéma d'architecture logique et réseau ;
- Inventaire des équipements, numéros de série, garanties et contrats associés ;
- Configuration des VLAN, règles principales, adressage et routage ;
- Documentation des hyperviseurs, stockages, NAS et sauvegardes ;

- Documentation de la solution de cybersécurité ;
- Procédures de sauvegarde, restauration, PRA et tests ;
- Procédures de maintenance, supervision et escalade ;
- Documentation de l'antispam ;
- Comptes rendus de recette, tests et transfert de compétences.

3.6 RECOMMANDATIONS

Le titulaire devra privilégier une architecture simple à administrer, documentée, sécurisée, évolutive et cohérente avec les compétences internes de l'établissement. Les solutions trop complexes, insuffisamment documentées ou dépendantes d'un mode d'exploitation opaque seront écartées.

La continuité de service pendant la migration est une exigence majeure. Toute opération susceptible d'entraîner une interruption devra être planifiée, validée par l'établissement et accompagnée d'un plan de retour arrière.

7. ANNEXES TECHNIQUES

Les documents suivants devront être produits ou mis à jour dans le cadre du marché.

Ils devront être produits pendant la phase de cadrage puis finalisées à la recette.

1. Inventaire détaillé de l'existant.
2. Schéma réseau logique cible.
3. Schéma d'implantation physique dans les baies.
4. Plan de migration et plan de retour arrière (le cas échéant).
5. Plan de sauvegarde et de restauration.
6. Plan de tests PRA.
7. Dossier de sécurité et matrice des accès.

8. DESCRIPTIF MATERIEL EXISTANT

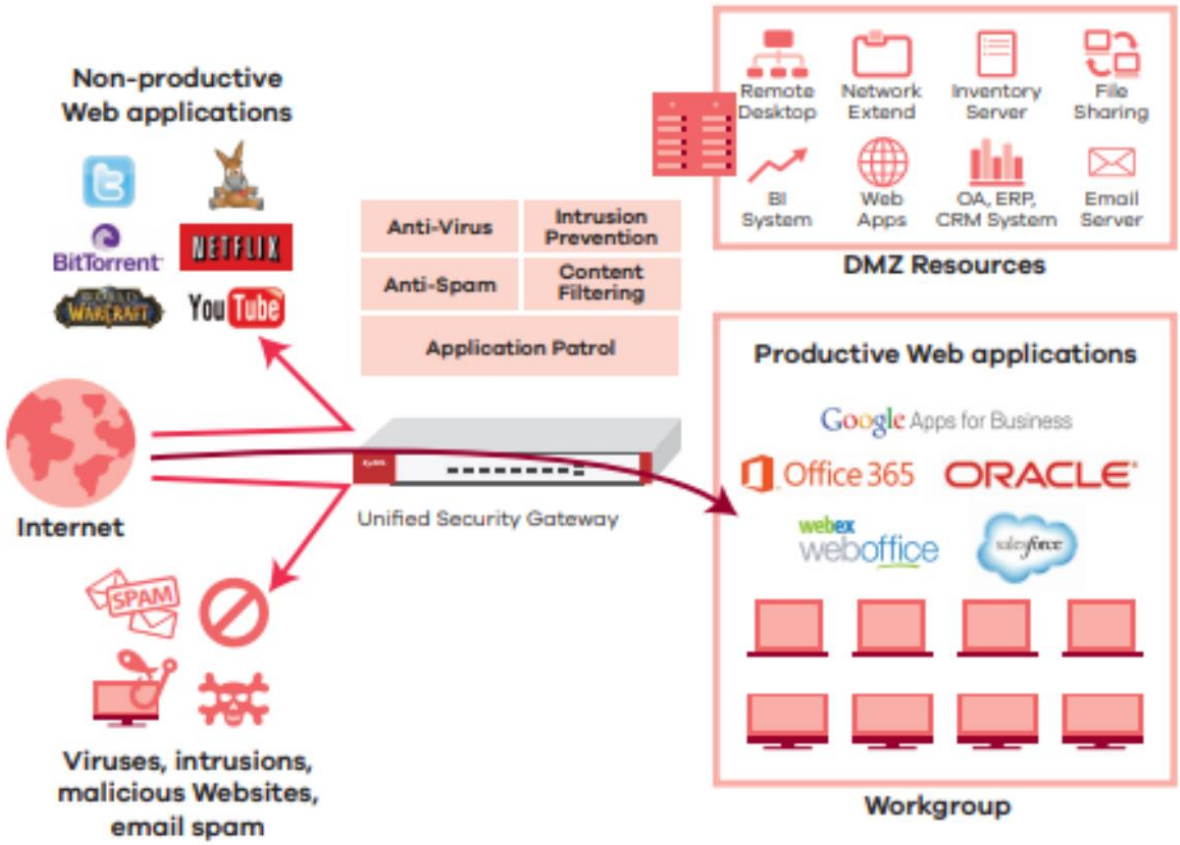
Firewall physique & suite logiciel UTM

Un cluster de 2 Firewall ZYXEL USG FLEX 500.

- Haute disponibilité avec bascule instantanée.
- VPN SSL intégré 150 utilisateurs.
- Contrôleur Wifi intégré avec segmentation de VLAN (public / privé).
- Composants intégrés :
    - Nombre max de connexions TCP simultanées > 1 Million.
    - Débit UTM 800 Mb.
    - Anti-Malware.
    - IPS (IDP).
    - Application Patrol (gestion des applications autorisé / interdites).
    - Filtrage web.
    - SecuReporter Premium.

L'EPAEM souhaite conserver ce matériel comme contrôleur pour la gestion du Wifi actuellement en place.





Contrôleurs wifi et bornes

Contrôleur géré via le cluster de 2 Firewall ZYXEL USG FLEX 500 (voir ci-dessus).
Licence complémentaire 16 AP WIFI ZYXEL.

Bornes Wifi Zyxel référence WAC6503D-S liaison filaire avec les contrôleurs (RDC et R+1).



Switch layer 3 - cœur de réseau

1 HPE ARUBA 2530-48G POE+, 10 Gb, 48 ports.



SWITCH Layer 2

6 HPE Aruba 2530-48G-PoE+ - Commutateur - Géré - 48 x 10/100/1000 (PoE+) + 4 x Gigabit SFP.



Socle hyperviseur de production

2 **HPE ProLiant DL380 Gen10,** serveur rack 2U polyvalent à deux alimentations redondantes.
2 CPU physiques de la gamme intel Xeon Silver 4215R soit 16 cores / 32 threads. Connectiques « Full Fibre » vers le LAN à 10 GB et réseau I-scsi dédié au VSAN à 2x25 GB/S.
192 Gb RAM ECC.



VSAN - baie stockage production

1 **HPE ProLiant DL380 Gen10,** serveur rack 2U polyvalent à deux alimentations redondantes.
14 x SSD d'une taille unitaire de 1TB dont 1xSSD au Hot Spare, ce qui donne une capacité utile en ligne de 12 TB.



PRA hyperviseur & VSAN

1 **HPE ProLiant DL380 Gen10,** serveur rack 2U polyvalent à deux alimentations redondantes.
14 hdd SATA de 1 TB unitaire, capacité de 12 tB avec Hot Spare et Raid 5.



NAS - backup matériel

2 NAS Synology RS241+, avec pour chaque serveur NAS 6xHDD 6TB unitaire à 7.2KIRONPORT PRO.
Capacité utile de 24 TB en Raid 5 avec Hot Spare.
Nas interne : carte 10 GB LAN avec module SPF+ Fibre vers cœur de réseau.

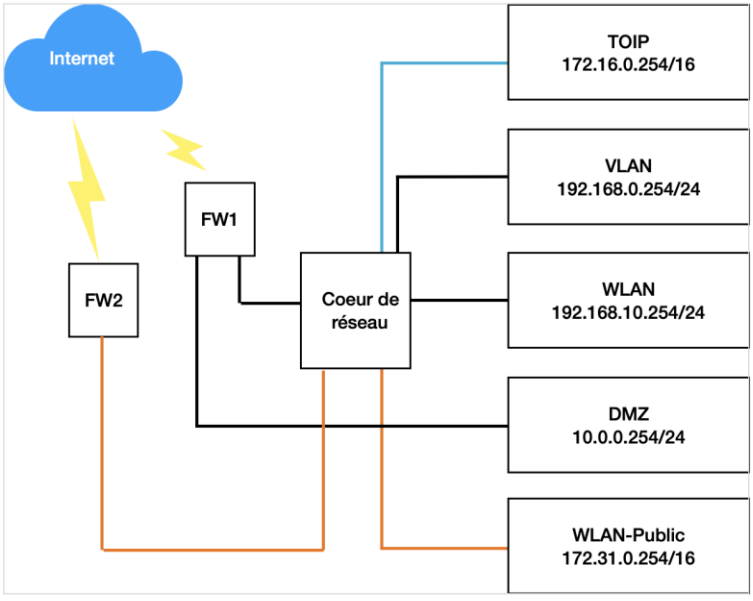


Onduleurs

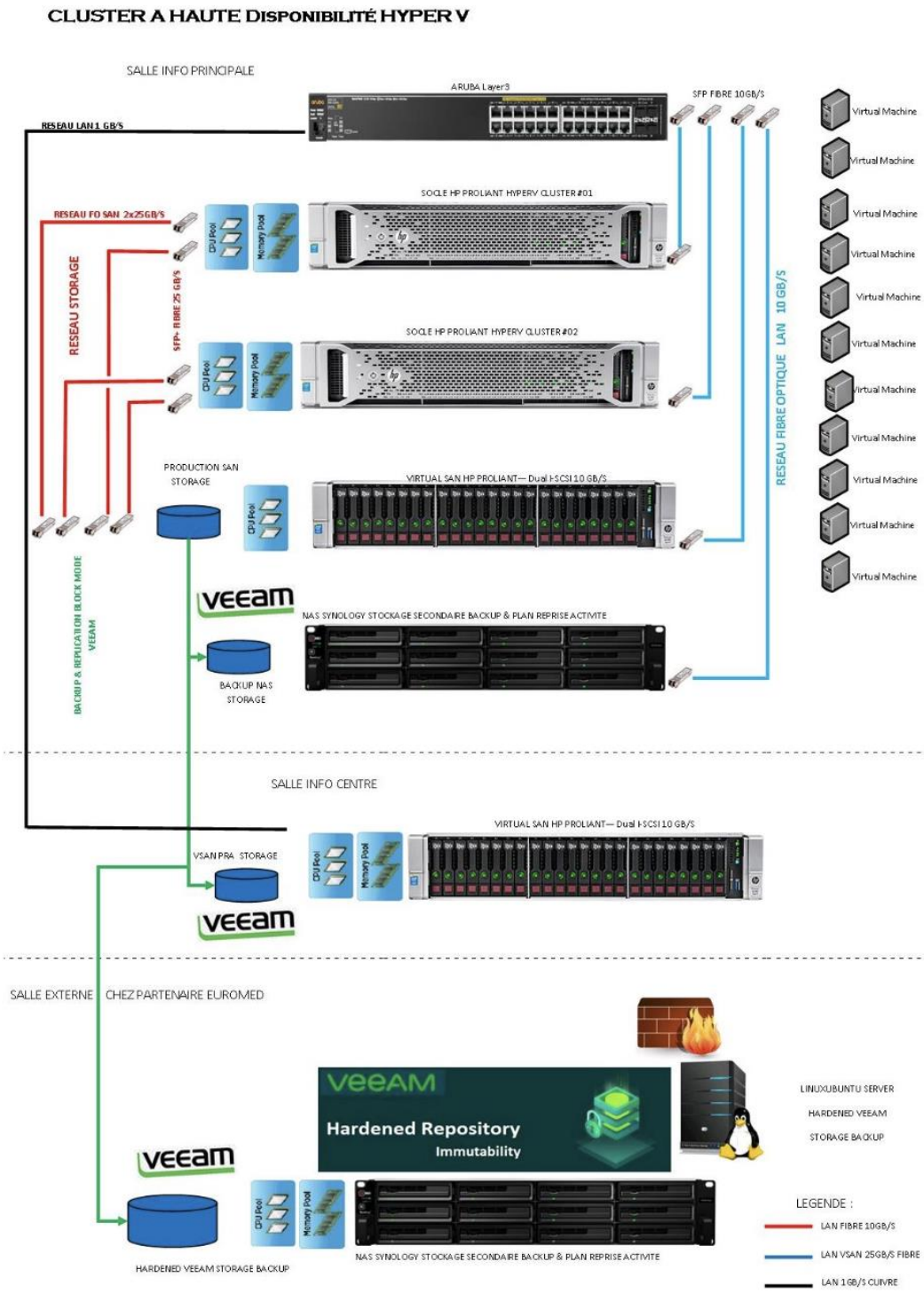
4 onduleurs NITRAM OSL3000 2U rack 19" 3 kVA. (3 R+1, 1 RDC).
Puissance unitaire de 3000 VA / 2700W. Les batteries Hot Swap (6).



Schéma réseau simplifié



Infrastructure



Salles serveur Astrolabe

R+1 : 3 baies dans salle climatisée.

Production + Backup



Distribution réseau



FW + Cœur de réseau



RDC : PRA

