AGENCE POUR LA SECURITE DE LA NAVIGATION AERIENNE EN AFRIQUE ET A MADAGASCAR

PLAN DES SERVICES ET EQUIPEMENTS 2023-2027

Projet N°2919 NPE 926050 - Mise à niveau de l'infrastructure IT

ACQUISITION D'UNE SOLUTION DE SAUVEGARDE

Cahier des Clauses Techniques Particulières

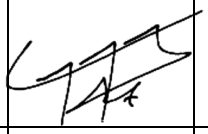
ASECNA Direction Générale *32-38, Avenue Jean Jaurès, BP 3144 - Dakar SENEGAL*
Tel : +221 33 869 51 37 - Secrétariat DTI Courriel : ***aos@asecna.org***, site : ***www.asecna.aero***

HISTORIQUE DU DOCUMENT

VERSION	DATE	DESCRIPTION DE L'EVOLUTION	OBSERVATIONS
V1	20/06/2025	Création du document	
V2	04/08/2025	Mise à jour des spécifications techniques	

NOTE IMPORTANTE : Toute nouvelle version annule et remplace la version précédente qui doit être détruite ou portée clairement sur la page de garde la mention manuscrite *VERSION PERIMEE.*

MAITRISE DU DOCUMENT

MAITRISE DU DOCUMENT				
	Nom	**Fonction**	**Visa**	**Date**
Rédacteurs	MALIKI Yazid	Cadre Supérieur Admin Système et Bases des Données		14-08-25
	SOILIH Rashid	Cadre Supérieur Réseaux Informatiques		16-08-25
	SAID NAFFION Rahim	Cadre Supérieur Réseaux Informatiques		16-08-25
Vérificateurs	TALEB Teneighmiche	DTIDIR		18-08-25
	TSHIMANGA née ZOUNGARANI Flora Mathilde	DTIDI		18 août 2025
Approbateur	AROUNA Touré Rahimi	DTID		18 août 2025

LISTE DE DISTRIBUTION	
DESTINATAIRES :	DTIDAM

AMPLIATAIRES :	

Table des matières

INTRODUCTION

I. Objectif du document

Le présent document constitue le Cahier des Clauses Techniques Particulières du projet d'acquisition d'une Appliance de sauvegarde par l'ASECNA. Le document a pour objet la mise en place d'une solution complète de sauvegarde, reposant sur une infrastructure résiliente, destinée à protéger les systèmes et les données sensibles de l'Agence.

II. Objectifs du projet

À ce jour, l'ASECNA ne dispose d'aucune solution de sauvegarde centralisée pour ses machines physiques, ses environnements virtualisés et ses données sensibles. Face aux antécédents de cyberattaques subis, cette situation représente un risque élevé pour la continuité des activités et la sécurité des données.

Ce projet vise donc à mettre en œuvre une solution de sauvegarde robuste permettant, en cas de perte de données ou d'incident critique, une restauration rapide, fiable et sécurisée. Dans son élan continu de la modernisation de son infrastructure informatique, l'ASECNA souhaite :

- Améliorer la disponibilité des serveurs et des données ;
- Faire évoluer sa politique de protection et de sécurisation des données informatique ;
- Améliorer la mobilité des utilisateurs et de leurs données ;
- Concrétiser son plan de continuité et de reprise d'activité ;
- Développer une plus grande souplesse pour gérer l'évolution des besoins du SI.
- Garantir la sauvegarde automatique et planifiée de l'ensemble des serveurs physiques et virtuels.
- Mettre en place une infrastructure répartie sur deux sites : un site principal de production et un site secondaire pour la réplication des sauvegardes).
- Permettre la sauvegarde de données provenant de sites distants (autres représentations connectées via WAN/VPN).
- Prévoir une sauvegarde externe vers Microsoft Azure, pour assurer une conservation hors site.
- Offrir des mécanismes de restauration rapide (fichiers, machines virtuelles, configurations complètes).

Tout cela en s'appuyant sur une organisation claire, transparente, optimale et éprouvée.

Ce document présent l'ensemble des spécifications techniques des services qui devront être disponibles dans la plateforme cible. Cette dernière devra être sous forme d'un cloud privé qui sera mis en œuvre à la Direction Générale de l'Agence et dans un site backup.

III. Objectifs Opérationnels

Pour mener à bien ce projet de modernisation et d'adaptation, il est nécessaire de définir sa finalité :

Sur le plan économique :

- ✓ Maitriser les coûts liés au stockage de données.

Sur le plan de la gestion du stockage de données :

- ✓ Consolider et optimiser l'espace de stockage de données ;
- ✓ Garantir la sauvegarde et la restauration des données ;
- ✓ Améliorer la gestion, la protection et la sécurité des données ;
- ✓ Mettre en place un Plan de Reprise d'Activité (PRA) ;
- ✓ Mettre en place un Plan de continuité d'Activité (PCA).

Sur le plan des applications et services :

- ✓ Garantir la reprise d'activité et des services après un incident ou un sinistre ;

CONTEXTE DU PROJET

I. Présentation de l'ASECNA

L'Agence pour la Sécurité de la Navigation Aérienne en Afrique et à Madagascar (ASECNA) est un établissement public à caractère multinational. Elle est dotée de la personnalité juridique et jouit d'une autonomie financière. Elle regroupe 18 Etats qui sont : Bénin, Burkina Faso, Cameroun, Centrafrique, Congo, Côte d'Ivoire, France, Gabon, Guinée Equatoriale, Guinée Bissau, Madagascar, Mali, Mauritanie, Niger, Rwanda, Sénégal, Tchad, Togo et Union des Comores.

L'ASECNA est implantée sur vingt-sept (27) sites principaux :

- Une Direction Générale, à Dakar au Sénégal, repartie sur quatre (04) sites : Jean Jaurès (en ville), Yoff, SAN MARCO à Yoff et Almadies.
- Dix-sept (18) Représentations : Bénin, Burkina Faso, Cameroun, République Centrafricaine, Congo, Côte d'Ivoire, Gabon, Guinée Equatoriale, Guinée Bissau, Madagascar, Mali, Mauritanie, Niger, Sénégal, Tchad, Togo, l'Union des Comores, Rwanda ;
- Trois (03) écoles : ERNAM (Dakar Sénégal), ERSI (Douala Cameroun) et EAMAC à Niamey (Niger) ;
- Trois (03) Délégations respectivement en Europe (Paris), auprès de l'Organisation de l'Aviation Civile Internationale (OACI à Montréal) et à l'Union Africaine (Addis-Abeba).

L'ASECNA assure une mission de service public de sécurité de la navigation aérienne et de la météorologie aéronautique.

II. Description de l'existant

L'ASECNA dispose pour ses besoins de fonctionnement d'un panel de plus d'une centaine de serveurs et près de 4000 PCs tout cela interconnectés via un réseau WAN et plusieurs réseaux LANs.

II.1. Infrastructure réseaux

Le siège de l'ASECNA à Dakar Yoff est le site principal de l'infrastructure réseau de l'Agence. Il héberge les applications, les différents serveurs de production et d'exploitation. Il agrège tous les accès en provenance des autres sites de l'Agence et à destination des applications et services localisés au siège.
Le site de Dakar Ville héberge certaines applications et constitue le site de backup de l'organisme pour les applications et serveurs existants.

Plusieurs centaines d'utilisateurs sont physiquement localisés à Yoff, Jean Jaurès et Almadies. Et ces utilisateurs accèdent aux applications au travers du réseau local LAN ou élargi (pour les utilisateurs de Dakar Ville) la liaison fibre de 200 Mo reliant les deux sites (Yoff et Ville) avec un backup VPN de 50Mbs.
Le site de YOFF est relié aux sites de l'ERNAM, de SAN MARCO et celui des Almadies par fibre optique d'une capacité de 1Gbps. Toutes les autres représentations (à l'exception de la Représentation du Sénégal reliée par fibre optique) sont connectées au site de Yoff via des liaisons satellitaires et des liaisons VPN.

II.2. Cartographie des serveurs existants du Siège

Ci-dessous la liste des serveurs et des applications existants sur le site principal de la Direction Générale de l'ASECNA à YOFF.

II.3. Serveurs physiques au Siège à Yoff

N°	Nbr de serveur	CPU	Mémoire	Stockage	OS	Plateformes/Services	Interfaces
1	2	4 sockets/20cores	512 Go	5 To	Windows server 2016/Datacenter	Hyper-V	GbE, 10GbE
2	5	2 sockets/08Cores	64 Go	3 To	Windows server 2016/Datacenter	Hyper-V	GbE
3	4	4 Sockets/18Cores	128 Go	5To	Windows server 2012 R2 Standard	Hyper-V	GbE
4	6	2 sockets/6Cores	64Go	2 To	Windows server 2012 R2 Standard	Hyper-V	GbE
5	2	3 sockets/6Cores	128 Go	2 To	Windows server 2012 R2 Standard	Hyper-V	GbE
6	1	2 sockets/6Cores	48 Go	4 To	Windows server 2012 R2 Standard	Hyper-V	GbE
7	2	4 sockets/20cores	512 Go	5 To	Windows server 2012 Datacenter	Hyper-V	GbE, 10GbE
8	3	2 sockets/6Cores	128 Go	2 To	Windows server 2012 R2 Standard	Hyper-V	GbE
9	1	2 sockets/6cores	64 Go	2 To	Windows server 2012 Datacenter	Hyper-V	GbE, 10GbE
10	1	2 sockets/6Cores	48 Go	4 To	Windows server 2012 R2 Standard	Hyper-V	GbE
11	2	4 sockets/20Cores	64 Go	4 To	Windows server 2012 Datacenter	Hyper-V	GbE, 10GbE
12	1	2 sockets/6Cores	64Go	5To	Linux Debian	-	GbE
20	2	2 sockets	384 GO	1.2 TB x4	Oracle Linux 7	OVM	GbE
21	2	2 sockets	512 GO	18 TB x 6	Oracle Linux 8	KVM	GbE

II.4. Stockages physiques au Siège à Yoff

N°	Nbr de Appliance	Stockage	Type de RAID	Interfaces
1	2	15 To -Hybride	RAID 10, 6	GbE, 10GbE
2	2	40 To-Sata	RAID 10, 6	GbE
3	1	30 To-Full flash	RAID 10, 6	GbE, 10GbE
4	4	84TB		GbE

SPECIFICATIONS DE L'OFFRE DE SERVICES

I. Prestations attendues

Ce chapitre prescrit la consistance des travaux à réaliser dans le respect des spécifications techniques associées.

Lors de la visite obligatoire des sites avant la proposition de son offre, le Soumissionnaire vérifiera les informations fournies dans ce document. A travers les visites de sites qui seront organisés à cet effet, il devra les compléter afin de tenir compte de tous les aspects pour proposer une offre la plus complète possible. Le soumissionnaire ne saura en aucun cas se prévaloir ultérieurement des éventuelles omissions ou erreurs

Le Soumissionnaire doit fournir des prestations suivantes :

- Fournir, installer et configurer la solution dans l'environnement de production ;
- Tester et valider la plateforme en production ;
- Surveiller la plateforme en production ;
- Former les ingénieurs et techniciens de l'ASECNA ;
- Réaliser un transfert de compétence aux ingénieurs et techniciens de l'ASECNA ;
- Faire la recette site de la solution déployée ;
- Fournir l'ensemble des livrables du projet ;
- Fournir la garantie sur l'ensemble des composantes de l'infrastructure installée ;
- Réaliser les maintenances préventives et curatives lors de la période de garantie ;
- Installer et configurer la PRA et la PCA entre les deux sites de type Siège ;
- Assister les ingénieurs ASECNA à distance à l'installation du troisième site PRA/PCA se trouvant dans la représentation ;
- Rédiger la procédure de backup en conformité avec les procédures ASECNA en vigueur ;
- Rédiger la procédure de PRA et de PCA en conformité avec les procédures ASECNA en vigueur
- Fournir une offre optionnelle pour la maintenance préventive et curative de l'infrastructure après la période de garantie.

II. Contrainte technique et exigence

Dans le cadre de sa stratégie de sécurisation de son système d'information, ASECNA envisage d'acquérir et d'implémenter une solution indépendante pour la gestion intégrée de sauvegarde et de restauration des données.

Le Soumissionnaire est invité à proposer une plateforme « matérielle et logicielle » dotée d'un haut niveau en matière de performance, de fiabilité, d'évolutivité, d'ouverture et de portabilité, ainsi qu'une gestion simplifiée des opérations de sauvegarde et de restauration.

Les principaux objectifs ciblés à travers l'acquisition d'une telle solution se déclinent comme suit :

1. Renforcer le niveau de sécurité du système d'information par la sauvegarde systématique de l'ensemble des ressources applicatives et informationnelles vitales de l'Agence ;
2. Assurer un haut niveau de disponibilité des données vitales à travers un système fiable de restauration automatique, rapide et sélectif ;
3. Avoir un système de sauvegarde qui apporte la protection des données sauvegardées contre les attaques virales et ransomware
4. Avoir un système de sauvegarde capable de détecter les anomalies lors des sauvegardes

5. Avoir un système de sauvegarde capable de faire le scan anti-Malware/antiviral sur les sauvegardes afin de vérifier l'intégrité des données sauvegardées
6. Permettre l'externalisation automatique des données par la réplication de toutes les sauvegardes
7. Avoir un système de sauvegarde permettant de respecter les SLA en termes de temps de sauvegarde et de restauration
8. Éviter les oublis et les erreurs qui peuvent être engendrés par la manipulation manuelle en prenant en charge les fonctions automatiques de sauvegarde et de restauration.

III. Périmètre des prestations

1. Acquisition, installation et mise en service de la plateforme de sauvegarde ;
2. Prestations de service autour de la plateforme proposée (Etude, Paramétrage, Recette) ;
3. Service d'implémentation du constructeur exigé
4. Transfert de compétence, assistance technique des administrateurs sur la nouvelle plateforme

Les caractéristiques minimales attendues sont les suivantes :

1. Le titulaire devra proposer une solution de sauvegarde et de restauration sur disque (Appliance et Logiciel de même marque)
2. La simplification de l'environnement grâce à des solutions intelligentes de sauvegarde (Appliance de sauvegarde et logiciel de sauvegarde)
3. Elle doit intégrer un logiciel antivirus pour protéger contre les attaques virales et ransomware
4. Elle doit fournir la capacité de détection et d'alerte d'anomalies lors des sauvegardes pour éviter de sauvegarder des données compromises
5. Elle doit avoir la capacité de faire le scan anti-malware/anti-viral après la sauvegarde et avant la restauration
6. Proposer un système de sauvegarde basé sur OS Linux
7. Proposer une meilleure protection efficace des environnements physiques, virtuels et cloud
8. L'accélération des sauvegardes avec les protocoles natifs aux Appliance de sauvegarde
9. La restauration instantanée des machines virtuelles et des bases de données
10. Elle doit prendre en charge la sauvegarde et la restauration, à partir et vers des environnements physiques, virtuelles et Cloud, avec la possibilité d'externaliser vers d'autres support de stockage tels que : disque, bande et Cloud, et ce en assurant une compatibilité avec la majorité des systèmes d'opération tels que (VMware, Hyper V, Linux, IBM i, AIX, Solaris, Windows, ...etc.).
11. Elle doit être compatible avec Microsoft Azure, avec un stockage des données opéré exclusivement dans le tenant Azure de l'ASECNA
12. Elle doit offrir des temps de restauration courts
13. Elle doit permettre la sauvegarde distante de sites géographiquement séparés
14. Elle doit être administrable de manière centralisée
15. Les données ne doivent pas sortir du périmètre géographique défini sans autorisation
16. Elle doit offrir des fonctionnalités telles que la déduplication online, la réplication, la compression, le cryptage des données (in-flight et At-rest) et la gestion des disques.

IV. Plan de reprise d'Activité

Le Plan de Reprise d'Activité (PRA) du projet repose sur une infrastructure de production et de secours répartie sur les trois (3) sites principaux (deux Sites Siège et le Cloud publique d'azure) qui sont secours l'un de l'autre. Ainsi, chaque site héberge une infrastructure de production et est backup d'un autre site tant sur les données de production que de la sauvegarde.

V. Architectures et dimensionnements cible

V.1. Architecture globale

L'architecture cible repose sur deux (2) sites de type Siège : le site principal de Yoff (DGY) et le site secondaire de Ville (DGV). Chacun de ces sites sera équipé d'une appliance de sauvegarde locale dédiée, hébergée dans un local technique sécurisé. Les deux appliances assureront une réplication bidirectionnelle active, de façon à garantir la disponibilité croisée des données entre les deux sites.

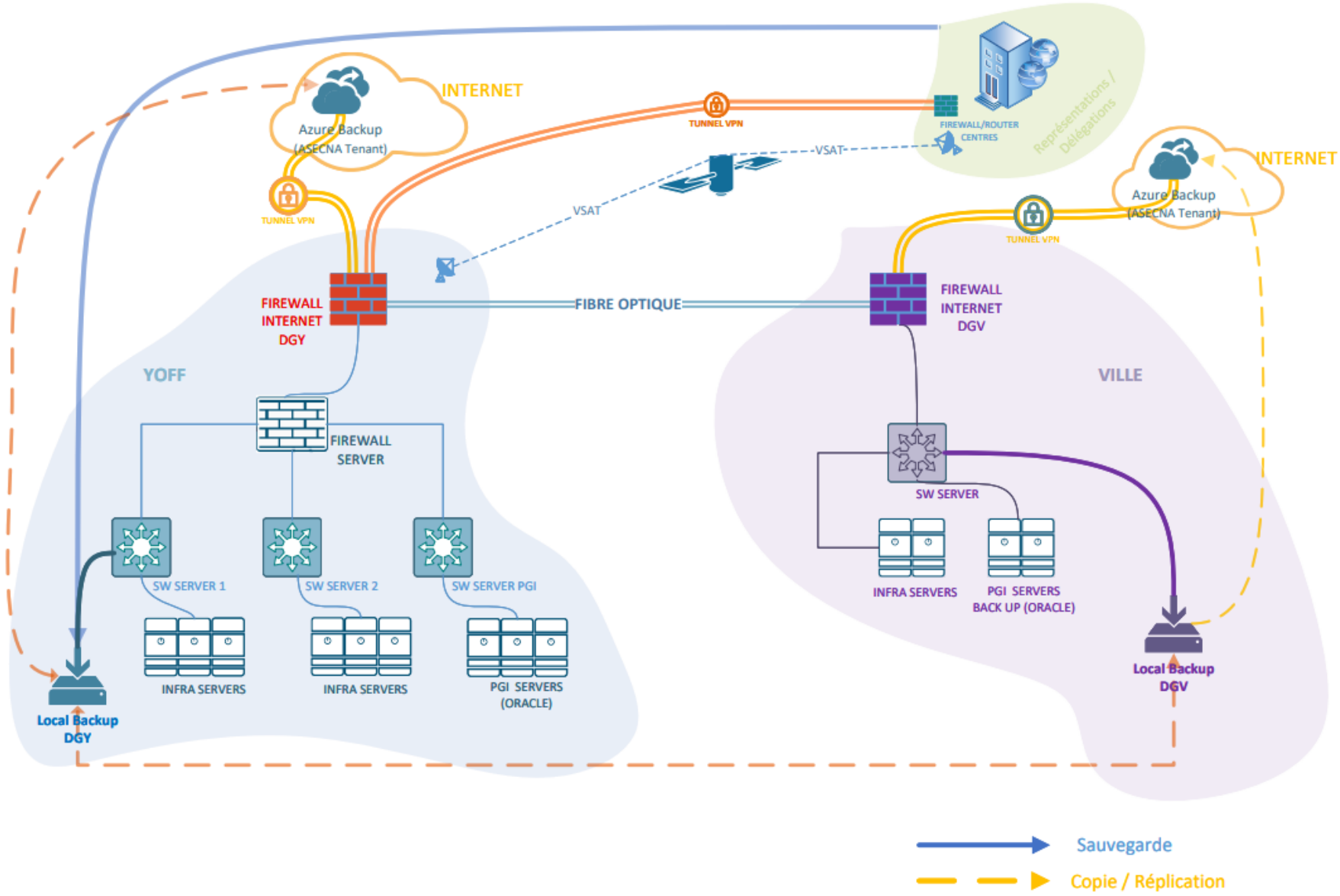
Le site de Yoff jouera le rôle de nœud principal de cette architecture, hébergeant les données critiques de production, tandis que le site de Ville fonctionnera comme réplica actif, capable de prendre le relais en cas d'indisponibilité du site principal.

En complément de cette infrastructure locale, une copie externalisée des sauvegardes sera hébergée dans le cloud Azure, via Azure Backup, afin de renforcer la résilience globale et de garantir la disponibilité des données même en cas de sinistre affectant les deux sites physiques.

Cette configuration vise à assurer une protection continue des données critiques, une reprise rapide en cas d'incident, ainsi qu'une conformité aux bonnes pratiques en matière de sauvegarde 3-2-1 (3 copies, sur 2 supports différents, dont 1 hors site).

- **Sites Siège :**
  - **Site de Yoff (DGY)**
  - **Site de Ville (DGV)**

Architecture cible de l'infrastructure de sauvegarde



V.2. Infrastructure de sauvegarde

La solution intégrée de sauvegarde doit prendre en charge la sauvegarde et la restauration, à partir et vers des environnements physiques, virtuels et Cloud, avec la possibilité d'externaliser vers d'autres support de stockage tels que : disque et Cloud, et ce en assurant une compatibilité avec la majorité des systèmes d'opération tels que Windows, Linux, Solaris, AIX, ESXi, AHV, Wintel, UX, ...etc.

L'éditeur de la solution doit être parmi les leaders sur le quadrant magique de Gartner des solutions de sauvegarde pour les deux dernières années.

Le Soumissionnaire devra proposer une solution de sauvegarde et de restauration sur disque (Appliance et Logiciel de même marque) avec des fonctionnalités telles que la déduplication, la réplication, le cryptage des données (in-flight et At-rest).

V.2.1. Caractéristique de l'infrastructure de sauvegarde pour les « Sites type Siège »

Logiciel de sauvegarde pour Sites type Siège

Le titulaire est invité à proposer une licence logicielle à la capacité de 10TB avec un support de **36 mois**. Le logiciel de sauvegarde doit être s'intégrer avec l'Appliance de sauvegarde, doit être préinstallé et provenir du même éditeur. Cette licence logicielle doit proposer les caractéristiques minimales ci-dessous :

CARACTERITIQUES MINIMALES PREVUES	VALEUR
Quantité Licence Logiciel	10 TB
Hétérogénéité	Prise en charge de tous types de serveurs (physique, virtuel, cloud), bases de données, hyperviseurs, applications et plates-formes Cloud.
Évolutivité	Haute performance, automatisation intelligente et gestion centralisée basée sur une architecture flexible et multi-niveaux.
Systèmes d'exploitation	Compatibilité avec des dizaines de versions de système d'exploitation serveur (OS), notamment Microsoft Windows, Linux et UNIX.
Systèmes virtuels	Compatibilité avec les principaux hyperviseurs, notamment **VMware, vSphere, Microsoft Hyper-V, AHV, RHV, OVM, KVM, OpenStack et Kubernetes**
Administration simplifiée et sécurisée	Interface utilisateur web simple avec workflows optimisés. Administration sécurisée basée sur les rôles avec contrôle d'accès et suivi d'audit.
Détection d'anomalies avec l'IA/le ML	Utilise l'intelligence artificielle pour détecter et notifier automatiquement les administrateurs si les données de sauvegarde changent de façon inattendue (Cryptage ransomware).

Scan Anti-Malware / Antiviral	Utilise le scan anti-malware pour vérifier l'intégrité des données sauvegardées après la sauvegarde et avant la restauration
Protection intégrée des données sauvegardées contre les attaques et intrusions	Intégration des fonctionnalités de détection d'intrusion et de protection contre les intrusions. Protection contre les attaques « zero-day », les menaces internes malveillantes et les ransomware
Détection d'anomalies avec l'IA/le ML	Utilise l'intelligence artificielle pour détecter et notifier automatiquement les administrateurs si les données de sauvegarde changent de façon inattendue (Cryptage ransomware).
Scan Anti-Malware / Antiviral	Utilise le scan anti-malware pour vérifier l'intégrité des données sauvegardées après la sauvegarde et avant la restauration
Bases de données et applications	Compatibilité avec les principales plateformes de bases de données et d'applications relationnelles, notamment **IBM DB2, Microsoft Exchange Server, Microsoft SQL Server, MySQL, Oracle, SAP, PostgreSQL**, etc.
Big data et plateforme hyperconvergée	Protection des environnements hyperconvergés et Big Data les plus exigeants (Nutanix, Hadoop, HBase, MongoDB, Cassandra)
Systèmes de stockage	Protection des données au niveau du système de stockage en intégrant diverses fonctionnalités de snapshot, de réplication et de NDMP.
Plateformes Cloud	Prise en charge de la sauvegarde et la restauration des charges de travail dans la plupart des environnements Cloud (AWS, **Azure**. Google, **OCI** etc..)
Récupération instantanée des machines virtuelles	Récupération des machines virtuelles et des bases de données en les démarrant directement à partir du disque de sauvegarde.
Accès Instantané aux données des machines virtuelles	Restauration des fichiers sur les machines virtuelles à partir d'un point précis en un seul clic et sans agent.
Récupération de Snapshots	Possibilité de ramener les systèmes à un point antérieur en récupérant un Snapshot matériel en ligne.
Restauration Bare Metal	Préparation rapide d'un système physique pour la restauration en évitant la configuration manuelle sur le même serveur ou sur un serveur d'un autre constructeur de serveur.
Conversion Infrastructure	Possibilité de faire du P2V, V2P, P2C, C2P, V2C, C2V

Récupération granulaire	Récupération granulaire via l'indexation du contenu des sources de données pour faciliter la restauration d'éléments spécifiques sans tentatives de restauration sans fin.
Réplication d'image automatique (AIR)	Les images de sauvegarde et les catalogues sont automatiquement répliqués via le réseau vers d'autres domaines sur site ou dans le Cloud conformément aux stratégies prédéfinies.
Réplication de snapshot	Les Snapshot matériel peuvent être répliqués automatiquement sur d'autres systèmes de stockage hors site.
Vault tape	Ejection automatique des bandes appropriées d'une bibliothèque robotique.
Gestion centralisée basée sur des politiques	Toutes les politiques de sauvegarde sont configurées à partir d'une console de gestion unique appliquée par le serveur maître.
Intelligent Automation	Détections automatiques des nouvelles machines virtuelles et des bases de données.
Self-Service	Fourniture d'une seule « vitrine » pour effectuer des sauvegardes en libre-service et des restaurations à l'aide d'interfaces personnalisées. Une seule instance peut enregistrer plusieurs locataires pour permettre une séparation sécurisée.
Rapports opérationnels	Identification rapide de l'utilisation des lecteurs de bandes, les taux de réussite et les zones non protégées et génération des rapports contextuels basés sur les secteurs d'activité, la géographie ou les applications dans un environnement hétérogène.
Surveillance et alerte sur données en cours de sauvegarde	Capacité d'alerter sur des anomalies détectées sur les données en cours de sauvegarde pour éviter de sauvegarder des données cryptées par un ransomware
Tendance et analyse à long terme	Prédiction de la consommation de stockage de sauvegarde en suivant les taux de croissance au fil du temps, y compris la pré- et post-déduplication, pour un suivi du retour sur investissement plus facile et des taux de déduplication.
Garantie et support	36 mois

Appliance de sauvegarde pour Sites Siège

Le titulaire est invité à proposer deux (2) Appliance de sauvegarde entièrement intégrées avec stockage extensible avec déduplication intelligente de bout en bout pour les environnements physiques, virtuels et Cloud. L'Appliance doit offrir une déduplication à la fois du côté client et du côté cible.

Le titulaire doit fournir deux (2) Appliance de sauvegarde avec stockage utile minimum de 140TB.

Les caractéristiques minimales de cette Appliance sont définies comme ci-dessous :

CARACTERITIQUES MINIMALES PREVUES	VALEUR
Format	Appliance physique rackable
Système d'exploitation	Basé sur Redhat Linux, optimisé, sécurisé et simplifié
Capacité de stockage utile de l'Appliance	140 TB
Quantité Licence Firmware de l'Appliance	140 TB
Nombre Unité du châssis	6U, rackable et doit respecter les normes internationales d'environnement
Extensibilité du stockage	Jusqu'à 429TB de capacité utile (possibilité de rajouter 6 extensions de stockage de 65TB)
Gestion du stockage	Stockage géré par Veritas Volume Manager (VxVM) et présenté au système d'exploitation via Veritas File System avec l'intégrité des données
Rôles fonctionnels multiples	Déploiement en tant que serveur maître, serveur de médias ou les deux
Architecture Zero Trust	Solution basée sur les principes Zero Trust avec une sécurité en couches (système d'exploitation renforcé, isolation des conteneurs, IPS/IDS intégré, stockage WORM intégré indélébile/immuable validé par Cohasset).
Protection intégrée des données sauvegardées contre les attaques et intrusions	Intégration des fonctionnalités de détection d'intrusion et de protection contre les intrusions. Protection contre les attaques « zero-day », les menaces internes malveillantes et les ransomware
Détection d'anomalies avec l'IA/le ML	Utilise l'intelligence artificielle pour détecter et notifier automatiquement les administrateurs si les données de sauvegarde changent de façon inattendue (Cryptage ransomware).
Scan Anti-Malware / Antiviral	Utilise le scan anti-malware pour vérifier l'intégrité des données sauvegardées après la sauvegarde et avant la restauration
Solution de stockage complète, immuable et indélébile	Intégrer une solution de stockage complète, immuable et indélébile pour défendre les données de sauvegarde contre les attaques ransomware
Contrôle d'accès basés sur les rôles et authentification multifactorielle	Au lieu de simplement exiger un mot de passe, utiliser la gestion des identités et des accès en mettant en œuvre un contrôle d'accès basé sur les rôles (RBAC) et une authentification à deux facteurs (ou authentification multifacteur, MFA) pour limiter l'accès à seules les fonctionnalités requises pour chaque personne et empêchent la prise de contrôle du compte en utilisant un seul identifiant

Protection ultime des machines virtuelles	Prise en charge VMware vSphere, Microsoft Hyper-V, AHV, RHV, OpenStack, Kubernetes, OVM, KVM
Accès Instantané aux données des machines virtuelles	Restauration des fichiers sur les machines virtuelles à partir d'un point précis en un seul clic et sans agent.
Optimisation du réseau étendu (WAN)	Taux de transfert jusqu'à 10 fois plus rapide pour les sauvegardes vers le Cloud et la réplication site to site
Fonctionnalité d'accélération de sauvegarde	Réalisation des sauvegardes complètes traditionnelles à la vitesse des sauvegardes incrémentielles
Réplication simple et rapide des Snapshot	Accélération de la gestion de la réplication des Snapshot et la récupération granulaire des données à partir de toute image de Snapshot répliquée
Optimisation de l'utilisation des ressources	Réduction du stockage de sauvegarde jusqu'à 50 fois et la consommation de bande passante jusqu'à 99%.
Options de déduplication flexibles	Déduplication à la source ou à la cible, en ligne ou post-processus
Élimination des serveurs de médias « Build-Your- Own »	Réduction des coûts d'exploitation, de la complexité et des frustrations liées à la création et au support des serveurs de médias
Réplication automatique d'image (AIR)	Réplication des images de sauvegarde sur un domaine distant pour la reprise après sinistre
Protection intégrée des données sauvegardées contre les attaques et intrusions	Intégration des fonctionnalités de détection d'intrusion et de protection contre les intrusions. Protection contre les attaques « zero-day », les menaces internes malveillantes et les ransomware
Passerelle Cloud hétérogène	Pris en charge de l'envoi de sauvegardes aux fournisseurs de stockage Cloud
Architecture matérielle résiliente	• Meilleure protection des données • Meilleure disponibilité du système • Redondance des composants remplaçables à chaud (alimentations redondantes, modules de ventilation et des disques de données enfichables à chaud)
Fonctionnalité d'AutoSupport :	Une surveillance du matériel garantissant que l'environnement de sauvegarde fonctionne de manière optimale, ce qui permet d'anticiper les besoins avant qu'ils ne deviennent des problèmes.
Fonctionnalité de sauvegarde pour Oracle	Activation de la sauvegarde et la restauration collaborative de la base de données
Récupération instantanée des bases de données Oracle	Récupération des bases de données Oracle en les démarrant directement à partir du disque de sauvegarde.
Disques	Disque SSD pour le système d'exploitation Disques SAS avec solution de gestion de stockage intégré pour les données
RAID	La prise en charge des configurations RAID 10, RAID 6 et RAID 1

Vitesse de sauvegarde	31TB /Heure minimum (dédupe à la cible) 124TB /Heure minimum (dédupe à la source)
Types de réplication	• « Plusieurs vers un » • « Un vers plusieurs » • « Plusieurs vers plusieurs »

Réplication chiffrée et compressée entre les systèmes	Oui
Externalisation	Supporte l'externalisation vers types FC de robotiques de sauvegardes
Certification	L'Appliance doit être certifié ENERGY STAR
Gestion	Console Java et Web centrale de gestion
Déduplication et compression être basées sur la cible et la source avec le même logiciel	Oui
Caractéristiques Matérielles Minimum	• 2 x Intel Xeon Silver 4314 CPUs @ 2.4GHz, 16 cores • 256GB extensible à 512GB of DDR4 RAM
Interfaces Réseaux	• Minimum Quatre (4) Ports 10Gb Ethernet • Minimum Six (6) Ports 10Gb/25Gb Ethernet FC • Interfaces Fibre Channel : Minimum Deux (4) Ports Fibre Channel à 16/32 Gbps
Ports	• 1 x port IPMI • 4 x USB 3.0
Garantie et support	36 mois

LIVRABLES DU PROJET

I. Formation sur le système Backup

Le prestataire est invité à former les équipes techniques à l'administration complète de la solution de sauvegarde, tant sur le plan logiciel (interface, stratégies, restauration, supervision, sécurité) que sur le plan matériel (gestion des appliances, support, monitoring physique, maintenance).

Les formations proposées doivent correspondre aux formations officielles du constructeur de la solution de sauvegarde proposée, avec support de cours et labs officiels, permettant d'assurer le niveau 2 de maintenance.

Ces formations qui feront l'objet d'évaluation doivent préparer à l'obtention des certifications requises. Le ou les formateurs doivent être hautement qualifiés et certifiés sur ladite solution.

Le prestataire prendra en charge les frais de formation des participants ;

La formation, devra être assurée dans un centre dédié agréé par l'éditeur.

Le prestataire doit indiquer, dans son offre, le détail relatif à la formation proposée entre autres le prérequis, la durée ainsi que le nom et le CV des formateurs.

Le ou les formateurs doivent être hautement qualifiés et certifiés sur ladite solution.

Population concernée pour la formation sur le Système Backup:

Nombre de participants	Formations	Nombre de bon de certification par examen	Observation
11	Administration professionnelle des plateformes de sauvegarde (matériel et logiciel)	**11**	- 08 Administrateurs Réseaux - 03 Administrateurs DBA

Contenu de la formation :

1. **Partie logicielle** :
   - Prise en main de la console de gestion
   - Création et gestion des politiques de sauvegarde
   - Planification, restauration, supervision
   - Sécurité, encryption, gestion des erreurs
   - Intégration cloud (Azure Backup)
2. **Partie matérielle** :
   - Présentation des appliances déployées
   - Surveillance des composants physiques (disques, interfaces)
   - Procédures de maintenance et de redémarrage sécurisé
   - Configuration réseau, notifications, logs matériels

Conditions logistiques et de prise en charge :

- **À la charge de l'ASECNA** :
  - Le **transport aller-retour** des participants vers le lieu de formation (billets)
  - Les **frais d'hébergement** (logement durant toute la durée de la formation)
- **À la charge du prestataire (formateur)** :
  - L'organisation matérielle et logistique complète de la session de formation (salles, équipements, support pédagogique)
  - La restauration en journée ainsi que la logistique de mobilité locale afférente à la formation seront assurées par le prestataire

II. Planning et méthodologie des prestations d'installation et déploiement

Les prestations d'installation et de mise en œuvre (incluses d'ailleurs dans les prix) de la plate-forme proposée doivent respecter la démarche suivante :

- Des réunions de cadrage et de suivi du projet ;
- Une phase d'implémentation et de configuration ;
- Une phase de migration ;
- Une phase de tests et de validation ;
- Une phase de surveillance ;
- Une phase de formation et de transfert de compétences.

II.1. Réunions de cadrage et de suivi :

Une première réunion de cadrage du projet doit être prévue pour concerter les objectifs ainsi que le planning du projet. Cette réunion doit être tenue, dans les 10 jours, au maximum, qui suivent l'ordre de service de commencement des prestations.
Un point d'avancement et de cadrage se fera de manière hebdomadaire pour le bon déroulement du projet.

II.2. Phase d'implémentation et de configuration

Lors de cette phase, le prestataire implémentera la solution sur l'environnement de production.

Tous les travaux d'installation, de déploiement et de mise en œuvre des produits objets de cet appel d'offres doivent être réalisés sans interruption ou dégradation des services opérationnels au niveau de l'ASECNA.

Le titulaire doit procéder à :

- La mise en rack des équipements ;
- L'interconnexion de tous les équipements ;
- La connexion des tous les équipements au réseau local ;

En termes de livrables, le titulaire doit fournir la liste non exhaustive ci-après :

- L'architecture physique de la solution de sauvegarde avec les noms des serveurs (physiques et virtuels) ainsi que leurs adresses et les interconnexions entre autres en format Visio ;
- Un dossier d'installation et de configuration. Il doit être complète et englobera toutes les étapes de l'installation à la mise en œuvre de la plate-forme ;
- La procédure de basculement d'un site à un autre ;
- Livrables connexes.

II.3. Phase de test et de validation

Le prestataire est amené à élaborer dans un premier temps un plan de test et un cahier de test (fonctionnement et performance) qui doit être validé par l'équipe de l'ASECNA.

Sur base de ce plan, des tests vont être réalisés par le titulaire en présence de l'équipe de l'ASECNA, pour vérifier le bon fonctionnement et les performances des différents équipements et logiciels installés et leur conformité aux besoins exprimés dans le présent cahier de prescriptions spéciales et lors de la phase préliminaire.

En termes de livrables, le titulaire doit fournir :

- Plan de test et cahier de test ;
- Résultats des tests.

II.4. Phase de formation et de transfert de compétence.

Cette phase sera consacrée à la formation du personnel de l'ASECNA, ainsi que le transfert toute compétence nécessaire pour gérer la plateforme mise en œuvre.

A la suite des transferts de compétences et des formations, les livrables de supports de formations et documents d'exploitation devront être fournis.

A partir de cette date, la phase de support après-vente devra couvrir les mises à jour et demandes d'assistances/modifications ou d'améliorations de l'ASECNA.

II.5. Dispositions générales

- Les interventions techniques devront tenir compte des contraintes en termes d'horaires (7h30 – 15H30).
- Les travaux nécessitant l'arrêt d'un service se feront hors des heures de travail et devront faire l'objet d'une planification rigoureuse.

III. Responsabilité et engagement du titulaire durant la période de garantie

Le soumissionnaire doit proposer une garantie de bon fonctionnement de tous les matériels et logiciels fournis, y compris les pièces de rechange, pendant une période de trois (03) ans à compter de la réception sur site.

La recette définitive ne doit être prononcée avant la levée de toutes les éventuelles réserves constatées lors du fonctionnement des équipements sur site.

III.1. Nature des prestations durant la période de garantie

III.1.1.Maintenance Hardware

- Maintenance curative pour :
  - Le dépannage des équipements matériels défectueux sur appel du maître d'ouvrage ;
  - La résolution des problèmes de paramétrage (tuning) des équipements sur appel du maître d'ouvrage.
- Mise à jour des firmwares planifiée en commun accord entre le maître d'ouvrage et le titulaire
- Un accès à un service de support client (Hot Line) pour pouvoir soumettre des questions relatives au paramétrage et de configuration des équipements fournis.

III.1.2.Maintenance des logiciels

- La livraison et installation des mises à jour majeures et mineurs des logiciels, après accord du maître d'ouvrage, et ce dès leur apparition. Le titulaire fournira également la documentation relative aux mises à jour. Dans le cas où une nouvelle version apportera de nouvelles fonctionnalités, le titulaire s'engage toujours à fournir la nouvelle version et sans coûts supplémentaires.

- La maintenance curative :
  - Sur appel du maître d'ouvrage en cas de dysfonctionnement, blocage ou dégradation des performances ;
  - Le titulaire s'engage à apporter son concours et tout son savoir-faire en collaboration avec l'éditeur pour assurer le bon fonctionnement des logiciels ;
  - La maintenance curative en cas d'incident.

Un accès à un service de support client en ligne (Hot Line) pour pouvoir soumettre des questions relatives au fonctionnement des logiciels fournis.

III.2. Centre d'appel

Pendant la période de garantie, le titulaire s'engage à mettre en place un centre d'appel (numéro de téléphone unique) à la disposition du maître d'ouvrage. Ce centre d'appels devra être aux standards internationaux devra assurer la prise en charge des appels des représentants du maître d'ouvrage et d'attribuer un numéro à chaque appel.

Ce centre d'appel doit être disponible chaque jour du lundi au vendredi de 07H30 à 15h30.

III.3. Enregistrement des appels par le maître d'ouvrage auprès du titulaire

Toutes les pannes ou anomalies constatées par le Maître d'Ouvrage, pourront être signalé au Titulaire par l'un des moyens suivants :

- Un appel téléphonique ;
- Une demande d'intervention écrite communiquée au technicien relevant du prestataire s'il se trouve sur place ;
- Une correspondance ;
  Ainsi titulaire remettra au maître d'ouvrage
- Un numéro de téléphone unique ;
- Une adresse mail ;

III.4. Remise en état de l'équipement/logiciel en panne sur site

Par remise en état, il est entendu la remise en service du matériel via :

- Pour les incidents hardwares
  - Soit un procédé de **réparation** sur site ;
  - Soit un **remplacement provisoire** de l'équipement défectueux par un équipement équivalent dont les performances seront validées par le maître d'ouvrage.

- Pour les incidents logiciels
  - Soit via un procédé de **rectification** sur site ;
  - Soit un procédé de **correction temporaire** ou de solutions d'urgence de contournement si la rectification définitive nécessite un délai plus long.

III.5. Réparation en atelier

- Pour les incidents hardwares

Quand la réparation nécessite le retour en atelier du Titulaire, le matériel défectueux devra être récupéré pour réparation et retourné au lieu de son exploitation par les services du Titulaire et à sa charge. Les frais de transport éventuels d'un équipement pour réparation, dans les ateliers du titulaire, sont à la charge de ce dernier.

- Pour les incidents logiciels

Lorsque **la rectification définitive** exige un délai long de mise en œuvre qui risquent de gêner l'exploitation, le titulaire est tenu d'apporter une solution dans les délai impartis en collaboration avec l'éditeur pour assurer le bon fonctionnement du logiciel.

III.6. Remplacement définitif des équipements

Lorsque l'équipement en panne ne peut pas être réparé dans le délai de **10 jours**, le titulaire doit procéder à son **remplacement définitif** par un équipement de **même marque et performances au moins égales** à celles de l'ancien. Un PV de remplacement définitif sera établi entre le maître d'ouvrage et le titulaire.

III.7. Fiche d'intervention

A la fin de chaque intervention, le Titulaire doit établir une **fiche d'intervention** qui porte sur les tâches effectuées. Cette fiche, **datée et signée** par les représentants du Maître d'ouvrage et du Titulaire, doit indiquer la date et l'heure exacte d'achèvement des travaux réalisés par le Titulaire et **doit être communiquée au Maître d'ouvrage**.

La date de fermeture des appels (date de résolution de l'incident) sera la date d'achèvement mentionnée sur la fiche d'intervention. Si la fiche d'intervention est non datée, la date de fermeture sera la date à laquelle le maître d'ouvrage a fermé l'appel au niveau de son système de gestion des incidents.

III.8. Délais

Le titulaire s'engagera à respecter les délais suivants :

Délai d'intervention	Délai de remise en état	Délai de réparation en atelier
2 heures	24 heures	15 jours pour les incidents hardwares 07 jours pour les incidents logiciels

NB : les délais ci-dessus sont comptés à partir de l'heure de l'enregistrement d'appel auprès du titulaire.

IV. Qualification prestataire

NB : L'ASECNA se réserve le droit de vérifier par des moyens qui lui seront propres l'exactitude de toutes les informations transmises par le soumissionnaire.
Les conditions minimales à respecter par le soumissionnaire sont les suivantes :

- ✓ Être certifié et reconnu par les constructeurs et éditeurs des différentes solutions qui seront mises en œuvre dans le dossier. A cet effet, le soumissionnaire joindra à son offre une attestation d'approbation délivré par le fabricant.

- ✓ Avoir exécuté au cours des trois (03) dernières années au moins un (01) marché similaire sur des infrastructures de sauvegarde de même envergure en termes de dimensionnement (avec une architecture multisite). Les attestations de bonne exécution signées par les autorités contractantes concernées devront être fournies.

- ✓ Disposer des ressources techniques locales certifiées (CV et attestations de certifications fournis) sur les solutions à installer niveau expert et architecte.

FIN DE DOCUMENT