



تمويلكم
TAMWILCOM

APPEL D'OFFRES OUVERT NATIONAL
SUR OFFRES DE PRIX N°12/2024/SNGFE

**HEBERGEMENT ET ORCHESTRATION MANAGES DE
CONTENEURS INCLUANT LA GESTION DES CHARGES DE
TRAVAIL (WORKLOADS) ET L'AUTOMATISATION DES
DEPLOIEMENTS AU PROFIT DE LA SOCIETE NATIONALE
DE GARANTIE ET DU FINANCEMENT DE
L'ENTREPRISE(SNGFE)**

Cahier des Prescriptions Spéciales

En application de l'alinéa 1 paragraphe I-1 et l'alinéa a) paragraphe 3 de l'article 19 et de l'alinéa b) du paragraphe 3 de l'article 20 du Règlement des Achats de la SNGFE

Décembre 2024

SOMMAIRE

Chapitre I : Clauses Administratives et Financières	3
Article 1 : Objet de l'appel d'offres	3
Article 2 : Répartition en lots	3
Article 3 : Maître d'Ouvrage	3
Article 4 : Lieu d'exécution des prestations	3
Article 5 : Consistance des prestations	3
Article 6 : Pièces constitutives du marché	3
Article 7 : Référence aux textes généraux	3
Article 8 : Validité et date de notification de l'approbation du marché	4
Article 9 : Pièces mises à la disposition du Titulaire	4
Article 10 : Nantissement	4
Article 11 : Élection du domicile du Titulaire	4
Article 12 : Sous-traitance	5
Article 13 : Délai d'exécution du marché	5
Article 14 : Variation et caractère des prix	5
Article 15 : Cautionnements – Retenue de garantie	5
Article 16 : Assurances – Responsabilités	6
Article 17 : Propriété industrielle, commerciale ou Intellectuelle - Responsabilité contractuelle	6
Article 18 : Réception des prestations	6
Article 19 : Modalités de règlements	6
Article 20 : Pénalités pour retard	7
Article 21 : Retrait ou remplacement du personnel du titulaire	7
Article 22 : Droits de timbre et d'enregistrement	7
Article 23 : Confidentialité des renseignements	7
Article 24 : Lutte contre la fraude et la corruption	8
Article 25 : Résiliation du marché	8
Article 26 : Règlement des différends et litiges	8
Chapitre II : Clauses Techniques	9
Article 27 : Consistance des prestations	9
Article 28 : Autres dispositions	22
Article 29: Décomposition du montant global	26

Chapitre I : Clauses Administratives et Financières

Article 1 : Objet de l'appel d'offres

Le présent appel d'offres a pour objet l'hébergement et l'orchestration managés de conteneurs, incluant la gestion des charges de travail (workloads) et l'automatisation des déploiements, au profit de la Société Nationale de Garantie et du Financement de l'Entreprise (SNGFE).

Article 2 : Répartition en lots

Le présent appel d'offres concerne un marché en lot unique.

Article 3 : Maître d'Ouvrage

Le Maître d'Ouvrage du marché qui sera passé suite au présent appel d'offres est la SNGFE représentée par le Directeur Général Adjoint - Ressources.

Article 4 : Lieu d'exécution des prestations

L'exécution des prestations objet du présent appel d'offres se déroulera au niveau du siège central de la SNGFE sis au Centre d'affaires, Bd. Ar Ryad, Hay Ryad – Rabat.

Article 5 : Consistance des prestations

La consistance des prestations objet du présent appel d'offres est décrite dans le chapitre II relatif aux clauses techniques.

Article 6 : Pièces constitutives du marché

Les pièces constitutives du marché sont :

- L'acte d'engagement ;
- Le présent Cahier des Prescriptions Spéciales (CPS) - projet du marché - ;
- La décomposition du montant global ;
- Le cahier des clauses administratives générales applicable aux marchés d'études et de maîtrise d'œuvre (CCAG/EMO).

En cas de contradiction ou de différence entre les pièces constitutives du marché, ces pièces prévalent dans l'ordre où elles sont énumérées ci-dessus.

Article 7 : Référence aux textes généraux

Le Titulaire du marché est soumis aux textes suivants :

1. Le Règlement des Achats de la Société Nationale de Garantie et du Financement de l'Entreprise tel qu'approuvé par son Conseil d'Administration du 21 septembre 2023, ci-après désigné par l'expression « Règlement des Achats de la SNGFE » ;
2. Le Décret n° 2-16-344 du 17 chaoual 1437 (22 juillet 2016) fixant les délais de paiement et les intérêts moratoires relatifs aux commandes publiques ;
3. Le Dahir n° 1-15-05 du 19 Rabii II (19 février 2015) promulguant la loi n° 112-13 relative au nantissement des marchés publics ;
4. Le Décret n°2-14-272 du 14 rejeb 1435 (14 mai 2014) relatif aux avances en matière de marchés publics.
5. Le cahier des clauses administratives générales applicable aux marchés d'études et de maîtrise d'œuvre (CCAG/EMO).
6. Les textes de loi et les règlements en vigueur au Maroc ;
7. Tous les textes réglementaires ayant trait aux marchés de l'Etat rendus applicables à la date de signature du marché.

Le Titulaire devra se procurer ces documents s'il ne les possède pas et ne pourra en aucun cas exciper de l'ignorance de ceux-ci et se dérober aux obligations qui y sont contenues.

Article 8 : Validité et date de notification de l'approbation du marché

Le marché ne sera valable, définitif et exécutoire qu'après son approbation par le Directeur Général de la SNGFE.

L'approbation du marché doit intervenir avant tout commencement d'exécution.

En application de l'article 143 du Règlement des Achats de la SNGFE, la notification de l'approbation du marché doit intervenir dans un délai **maximum de soixante (60) jours** à compter de la date fixée pour l'ouverture des plis.

Article 9 : Pièces mises à la disposition du Titulaire

Aussitôt après la notification de l'approbation du marché, le Maître d'Ouvrage remet gratuitement au Titulaire, contre décharge de ce dernier, un exemplaire vérifié et certifié conforme de l'acte d'engagement, du cahier des prescriptions spéciales et des pièces expressément désignées comme constitutives du marché telles qu'indiquées ci-dessous ; à l'exception du cahier des prescriptions communes applicable et du cahier des clauses administratives générales relatifs au marché des études et maîtrise d'œuvre (CCAG/EMO).

Le Maître d'Ouvrage ne peut délivrer ces documents qu'après constitution du cautionnement définitif, le cas échéant.

Article 10 : Nantissement

Dans l'éventualité d'une affectation en nantissement du marché, il sera fait application des dispositions de la loi n° 112-13 relative au nantissement des marchés publics promulguée par le dahir n° 1-15-05 du rabii II (19 février 2015), étant précisé que :

1. la liquidation des sommes dues par le Maître d'Ouvrage en exécution du présent marché sera opérée par les soins du Directeur Général de la SNGFE ou son représentant ;
2. au cours de l'exécution du marché, les documents cités à l'article 8 de la loi n°112-13 peuvent être requis du Maître d'Ouvrage, par le Titulaire du marché ou le bénéficiaire du nantissement ou de la subrogation et sont établis sous sa responsabilité ;
3. lesdits documents sont transmis directement à la partie bénéficiaire du nantissement avec communication d'une copie au Titulaire du marché, dans les conditions prévues par l'article 8 de la loi n° 112-13 ;
4. les paiements prévus au marché seront effectués par l'ordonnateur, seul qualifié pour recevoir les significations des créanciers du Titulaire du marché ;
5. le Maître d'Ouvrage remet au Titulaire du marché une copie du marché portant la mention « exemplaire unique » dûment signé et indiquant que ladite copie est délivrée en exemplaire unique destiné à former titre pour le nantissement du marché.

Les frais de timbre de l'original du marché et de l'exemplaire unique remis au Titulaire sont à la charge de ce dernier.

Article 11 : Élection du domicile du Titulaire

A défaut d'avoir élu domicile au niveau de l'acte d'engagement, toutes les correspondances relatives au présent marché sont valablement adressées au domicile élu par le Titulaire, sis Maroc. En cas de changement de domicile, le Titulaire est tenu d'en aviser le Maître d'Ouvrage dans un délai de quinze (15) jours suivant ce changement.

Article 12 : Sous-traitance

Les conditions de sous-traitance sont celles prévues au niveau de l'article 151 du Règlement des Achats de la Société Nationale de Garantie et du Financement de l'Entreprise.

Si le Titulaire recourt à la sous-traitance dans les conditions prévues au niveau de l'article 151 du règlement précité, il est tenu de présenter au Maître d'Ouvrage les documents justifiant le paiement, par ses soins, des sommes dues au sous-traitant, au fur et à mesure de l'exécution des prestations sous-traitées.

Article 13 : Délai d'exécution du marché

Le présent marché sera conclu pour une durée de **douze (12) mois**, il prendra effet à compter de la date d'effet de l'ordre de service de commencement, il sera **reconduit tacitement** d'année en année, sans toutefois excéder **cinq (05) années**.

Le délai global pour la mise en place de la solution est de quinze (15) jours à compter de la date de commencement des prestations.

Nonobstant la reconduction du marché par période annuelle, le Maître d'Ouvrage pourra mettre fin au marché, après préavis écrit d'un (01) mois, notifié par lettre recommandée au titulaire.

Dans le cas où le titulaire désire mettre fin au marché, il est tenu d'en aviser la SNGFE par lettre recommandée quatre (04) mois avant l'échéance.

Article 14 : Variation et caractère des prix

Les prix de marché sont fermes et non révisables.

Le marché est à prix mixte.

Les prix mentionnés au niveau de la décomposition du montant global doivent tenir compte de l'ensemble des prestations auxquelles ils s'appliquent, non seulement tels que ceux-ci sont décrits dans la décomposition du montant global, mais aussi tels qu'ils doivent être effectivement exécutés pour aboutir à l'exécution des prestations demandées.

Les prix du marché sont réputés comprendre toutes les dépenses résultant de l'exécution des prestations objet du marché y compris tous les droits, impôts, taxes, frais généraux, faux frais et d'une façon générale toutes les dépenses qui sont la conséquence nécessaire et directe de l'exécution des prestations objet du marché.

Article 15 : Cautionnements – Retenue de garantie

- **Cautionnement provisoire :**

Le **cautionnement provisoire** est fixé à **quinze mille (15.000,00) dirhams**.

Le **cautionnement définitif** est fixé à **trois pour cent (3%)** du montant, toutes taxes comprises, initial du marché.

Le montant du cautionnement provisoire fixé ci-dessus reste acquis à la Société Nationale de Garantie et du Financement de l'Entreprise dans le cas où le Titulaire ne réalise pas son cautionnement définitif dans un délai de 30 jours suivant la date de la notification de l'approbation du marché.

Le cautionnement définitif sera restitué ou la caution qui le remplace libérée par la mainlevée délivrée par la SNGFE dans un délai maximum de trois mois suivant la date de la réception définitive des prestations.

Par dérogation au CCAG-EMO aucune retenue de garantie n'est demandée les prestations du marché.

Article 16 : Assurances – Responsabilités

Le Titulaire doit adresser au maître d'ouvrage, avant tout commencement de l'exécution du marché, les copies des polices d'assurance qu'il doit souscrire et qui doivent couvrir tous les risques inhérents à la réalisation du marché, et ce conformément aux dispositions de l'article 20 du CCAG-EMO.

Article 17 : Propriété industrielle, commerciale ou Intellectuelle - Responsabilité contractuelle

Le Titulaire assume une obligation de résultats : celui-ci indemniser le Maître d'Ouvrage pour tout dommage matériel résultant directement d'une faute prouvée du Titulaire, dans le cadre du marché.

Le Titulaire garantit formellement la SNGFE contre toutes les revendications des tiers concernant les brevets d'invention relatifs aux procédés et moyens utilisés, marques de fabrique, de commerce et de service.

Il appartient au Titulaire le cas échéant, d'obtenir les cessions, licence d'exploitation ou autorisation nécessaires et de supporter la charge des frais et redevances y afférentes.

Article 18 : Réception des prestations

Après exécution de la prestation de mise en place, et à la suite de la remise des livrables incombant à cette prestation, le Maître d'Ouvrage procède à son appréciation. Si le Maître d'ouvrage estime que la prestation de mise en place répond aux spécificités techniques décrites au niveau de ce cahier des prescriptions spéciale il prononcera la réception de cette prestation et établira un procès-verbal de réception.

Les autres prestations réalisées feront l'objet de procès-verbaux de réception provisoire partielle semestrielle, établis par la ou les personnes désignées à cet effet par le Maître d'Ouvrage.

La dernière réception provisoire partielle coïncide avec les réception provisoire et définitive du marché.

La réception définitive sera prononcée à la fin de l'exécution du marché reconductible.

Article 19 : Modalités de règlements

Le paiement des prestations sera effectué semestriellement et à terme échu, par virement au compte bancaire du titulaire, en appliquant aux prestations réellement exécutées et régulièrement constatées et suite aux réceptions définies à l'article 18 ci-dessus.

La facture à présenter par le Titulaire doit être conforme au modèle de la décomposition du montant global arrêtée en toutes lettres, certifiée exacte et signée par le Titulaire qui doit en outre rappeler son compte bancaire (RIB).

La facture doit être communiqué à la SNGFE en 3 exemplaires dans un délai ne dépassant pas 05 jours à partir de la date de réception des prestations, accompagnée du PV de réception signé conformément à l'article 18 du présent cahier des prescriptions spéciales. Toute facture ne respectant pas les conditions précédemment citées sera rejetée par la SNGFE.

Il sera tenu compte dans le règlement des montants des pénalités à appliquer.

Article 20 : Pénalités pour retard

A défaut d'avoir réalisé la mise en place de la solution dans les délais prescrits, il sera appliqué au Titulaire une pénalité par jour calendaire de retard de 1 ‰ (un pour mille) du montant initial du marché modifié ou complété éventuellement par les avenants.

Cette pénalité sera appliquée de plein droit et sans mise en demeure sur toutes les sommes dues au Titulaire.

L'application de ces pénalités ne libère en rien le Titulaire de l'ensemble des autres obligations et responsabilités qu'il aura souscrites au titre du présent marché.

Toutefois, le montant cumulé de ces pénalités est plafonné à dix pour cent (10 %) du montant initial du marché modifié ou complété éventuellement par des avenants.

Lorsque le plafond des pénalités est atteint, l'autorité compétente est en droit de résilier le marché après mise en demeure préalable et sans préjudice de l'application des mesures coercitives prévues par l'article 52 du CCAG-EMO.

Article 21 : Retrait ou remplacement du personnel du titulaire

1 – Sauf dans le cas où le Maître d'Ouvrage en aurait décidé autrement, aucun changement ne sera apporté au personnel du Titulaire. Si, pour des raisons indépendantes de la volonté du titulaire, il s'avère nécessaire de remplacer un des membres du personnel intervenant, le Titulaire fournira une ressource d'une qualification égale ou supérieure.

2 – Si le Maître d'Ouvrage n'est pas satisfait de la performance d'un membre de l'équipe ou découvre qu'un des membres du personnel s'est rendu passible d'un manquement sérieux ou est poursuivi pour crime ou délit, ou si il a des raisons suffisantes pour être non satisfait du niveau de compétence ou du comportement d'un des membres du personnel, le Titulaire devra alors, sur demande motivée du Maître d'Ouvrage, désigner immédiatement un remplaçant dont la qualification et l'expérience sont jugées acceptables par celui-ci.

3 – Le personnel désigné par le Titulaire, en remplacement conformément aux dispositions des clauses (1) et (2) ci-dessus, sera soumis à approbation écrite préalable du Maître d'Ouvrage. Le Titulaire prendra à sa charge tous les frais de voyage et autres résultant de ce retrait et/ou de ce remplacement. Il ne pourra soumettre des demandes de paiements au titre des coûts supplémentaires résultant du retrait ou remplacement du personnel.

Article 22 : Droits de timbre et d'enregistrement

Le Titulaire doit acquitter les droits auxquels peuvent donner lieu le timbre et l'enregistrement du marché, tels que ces droits résultent des lois et règlements en vigueur.

Article 23 : Confidentialité des renseignements

Le Titulaire sauf consentement préalable par écrit du Maître d'Ouvrage, ne communiquera le marché, ni aucune de ses clauses, ni aucune des spécifications ou informations fournies par le Maître d'Ouvrage ou en son nom et au sujet du marché, à aucune personne autre qu'une personne employée par le Titulaire pour l'exécution du marché. Les informations transmises à une telle personne le seront confidentiellement et seront limitées à ce qui est nécessaire à ladite exécution.

Tout document, autre que le marché lui-même, demeurera la propriété du Maître d'ouvrage.

Afin de garantir le secret, la sécurité et la confidentialité des données de la SNGFE, le Titulaire

s'engage à travers la signature d'un contrat de clause de confidentialité qui lui sera remis avant tout commencement d'exécution des prestations.

Article 24 : Lutte contre la fraude et la corruption

Il sera fait application des articles 29 et 162 du Règlement des Achats de la SNGFE.

Le Titulaire ne doit pas recourir par lui-même ou par personne interposée à des pratiques de fraude ou de corruption des personnes qui interviennent, à quelque titre que ce soit, dans les différentes procédures de passation, de gestion et d'exécution du marché.

Le Titulaire ne doit pas faire, par lui-même ou par personne interposée, des promesses, des dons ou des présents en vue d'influer sur les différentes procédures de conclusion d'un marché et lors des étapes de son exécution.

Les dispositions du présent article s'appliquent à l'ensemble des intervenants dans l'exécution du présent marché.

Article 25 : Résiliation du marché

En cas de résiliation du présent marché, il sera fait application des dispositions prévues au CCAG/EMO.

Article 26 : Règlement des différends et litiges

Si au cours de la réalisation du marché, des différends et litiges surviennent avec le Titulaire, les parties s'engagent à régler celles-ci dans le cadre des stipulations du CCAG/EMO.

Les litiges entre la SNGFE et le Titulaire sont soumis au Tribunal Administratif de RABAT.

Chapitre II : Clauses Techniques

Article 27 : Consistance des prestations

Les prestations objet du présent appel d'offres, comprennent la mise en place de services d'hébergement et d'orchestration managés de conteneurs, incluant la gestion des charges de travail (workloads) et l'automatisation des déploiements au profit de la SNGFE. Elles englobent également l'infogérance de la solution, en assurant sa supervision, sa maintenance proactive et sa gestion complète, ainsi qu'une assistance à la demande pour fournir un support technique réactif et adapté aux besoins spécifiques.

PRIX N° 1 : Services d'hébergement et d'orchestration managés de conteneurs, incluant la gestion des charges de travail (workloads) et l'automatisation des déploiements au profit de la SNGFE

I. Objectif :

La société Nationale de Garantie et du Financement de l'Entreprise compte héberger un Orchestrateur en mode managé et infogéré sur le cloud au Maroc, permettant la gestion de charges de travail (workloads), la gestion des services conteneurisés, l'automatisation des déploiements et garantissant la sécurité des données, répondant aux usages :

- Utilisation par les équipes développement pour le développement de nouveaux services ;
- Qualification / test d'intégration avec les applications existantes et les partenaires ;
- Déploiement des nouveaux services en production ;
- Déploiement du Site Web ;
- Publication et exposition des services de la SNGFE sur Internet ;

La « plateforme as a service (PAAS) » doit être installée au niveau de deux Data Center (REGION) sur le territoire Marocain certifié au moins :

- ISO 27001 ;
- « Tier III of Design » ou « Tier III Certification Constructed Facility ».

Le Titulaire s'engage formellement sur les performances de la solution fournie, à savoir :

- La capacité à délivrer le service attendu ;
- La disponibilité du système tel que précisé dans ce CPS ;
- Les temps de réponse ;
- La robustesse de la solution ;
- La sécurité de la solution ;
- Le respect des standards du marché ;
- La simplicité d'exploitation et d'administration de la solution proposée.

II. Exigences techniques

Dans ce qui suit, les exigences techniques minimales de la SNGFE liées à l'Orchestrateur sont listées :

1. Fonctionnalités générales et de base du moteur Kubernetes:

- La solution doit intégrer toutes les fonctionnalités de Kubernetes ;

- La solution doit disposer d'un Dashboard web imbriquant toutes les fonctionnalités de l'orchestrateur ;
- Gérer les containers de type Dockers ou autres types ;
- Utiliser un mode d'installation automatisé et simple ;
- Utiliser un mode de mise à jour de version automatisé et simple ;
- Ajouter des nœuds d'une manière automatisée et simple ;
- Possibilité de rajout de nœuds avec processeurs GPU ;
- Possibilité de rajout de nœuds avec processeurs Intel, AMD ou ARM
- Gérer les droits, restriction, authentification, etc... ;
- Capacité à provisionner des environnements logiciels rapidement ;
- La plateforme devant offrir plusieurs méthodes de connections : Via console web, Via Ligne de commande, Via REST API, Via SDKs.
- Déploiement rapide des solutions en production : le déploiement de la solution doit se faire en trente (30) jours à partir de la date de commencement des prestations ;
- Densification des infrastructures avec une augmentation des applications ;
- Scalabilité automatique face aux pics d'usage (développement/usage des applications) ;
- La solution proposée, doit être flexible et permettre le déploiement sur tout type d'infrastructure Cloud ou hybride ;
- Toute la solution, hardware et software, doit être gérée par un seul prestataire via la même interface et le même support éditeur ;
- Compatible avec la chaine DEV/SEC/OPS de la SNGFE ;
- La solution doit proposer des outils Dev/SEC/Ops intégrés ;
- La Solution doit disposer d'une vue développeurs simplifiés ;
- La solution doit être hébergée sur le territoire marocain. Le titulaire doit proposer une solution pour 3 environnements sur 2 sites, en voici les caractéristiques minimales :

Environnement	Site	Capacité minimale
PRODUCTION	Principal (6 nœuds)	1 Cluster Kubernetes : 24 Cores physiques(48vcpu), 96 GB de RAM, 6 TB de Block de Stockage
DISASTER RECOVERY	Secondaire (3 nœuds)	1 Cluster Kubernetes : 12 Cores physiques(24vcpu), 48 GB de RAM, 3 TB de Block de Stockage
DEVELOPPEMENT	Principal / Secondaire (1 nœud)	1 Cluster Kubernetes : 3 Cores physiques(6vcpu), 24 GB de RAM, 1TB de Stockage Block
LICENCE KUBERNETIES	Principal / Secondaire	INCLUE
MANAGEMENT		INCLUE

LIMITES SUR LES APPLICATIONS ET PODS		Pas de limite sur le nombre des applications, utilisateurs final et développeurs (basé sur la capacité)
MISE A L'ECHELLE AUTOMATIQUE		INCLUE
BASCULEMENT AUTOMATIQUE		INCLUE
STOCKAGE POUR LE BACKUP		20 TB de Stockage Objet au minimum
BACKUP AUTOMATIQUE		INCLUE
RESEAUX SDN		Ingress INCLUE ; Egress : INCLUE limité à 10T /Mois
LAN2LAN		Minimum 1GBPS
SERVICES		Moteur Kubernetes, Disaster recovery sur les regions, Développement, WAF et Loadbalancer, Firewall sur les regions, DDoS , Antivirus, Identity Access Management (IAM), Journalisation (logging), Monitoring, Scan de vulnérabilité.
REPRISE APRES SINISTRE DE LA PILE COMPLETE		INCLUE (DR)
CONFORMITE		LOI 05-20, 4/w/2022, 3/W/16 BKAM, DNSSI, PCI, FedRam, DISA, ISO, SOX ...
SECURITY CENTER GUARD		INCLUE la Surveillance en temps réel, Détection des menaces, Réponses automatisées, Conformité et bonnes pratiques, Tableau de bord centralisé
FORMATION		INCLUE
SUPPORT		24/7
		INFOGERANCE
ADMINISTRATION DES OS		INCLUE
ADMINISTRATION KUBERNETIES		INCLUE
ADMINISTRATION DU WAF, FIREWALL, IPS, LOGGING, MONITORING		INCLUE
ADMINISTRATION DU LOADBALANCER		INCLUE
GESTION DES UTILISATEURS		INCLUE
GESTION DE IAM et MFA		INCLUE
GESTION DES DNS ET CERTIFICATS		INCLUE
GESTION DES VPN		INCLUE
CREATION ET SUPPRESSION DES NOEUDS		INCLUE
SAUVEGARDE ET RESTAURATION		INCLUE

2. Architecture Cible

L'architecture cible repose sur un déploiement haute disponibilité et sécurisé de Kubernetes managé. Elle est conçue pour répondre aux besoins de production et de reprise après sinistre (DR), avec une redondance géographique entre deux sites. Voici les principaux éléments décrivant cette architecture :

a. Connexion On-Premises à la solution

- Intégration via **Connexion dédiée** ou un **VPN Site-to-Site**, permettant une connectivité sécurisée et à faible latence entre les infrastructures on-premises et la solution.

b. Multi-sites et Redondance

- **Région /Site 1 (Production) :**
 - Héberge les clusters Kubernetes en environnement de production et de développement, répartis sur différents **domaines de pannes (Zone de Défaillance)** pour assurer une tolérance aux défaillances matérielles.
 - Comprend des sous-réseaux publics et privés pour une segmentation réseau stricte.
- **Région / Site 2 (Disaster Recovery) :**
 - Implémente un cluster Kubernetes DR synchronisé avec le site principal via des mécanismes de réplication des données et des registres de conteneurs.
 - Maintient une architecture identique pour permettre une reprise complète en cas de sinistre.

c. Réseau et Sécurité

- **Réseau :**
 - Segmentation réseau via des sous-réseaux publics (Load Balancers) et privés (clusters Kubernetes).
 - Connexions inter-sites établies via **Network Peering** sécurisé.
- **Firewalls et WAF (Web Application Firewall) :**
 - Protection des applications accessibles publiquement contre les menaces.
- **Identity and Access Management :**
 - Gestion des accès avec des rôles et des permissions granulaires.

d. Kubernetes et Workloads

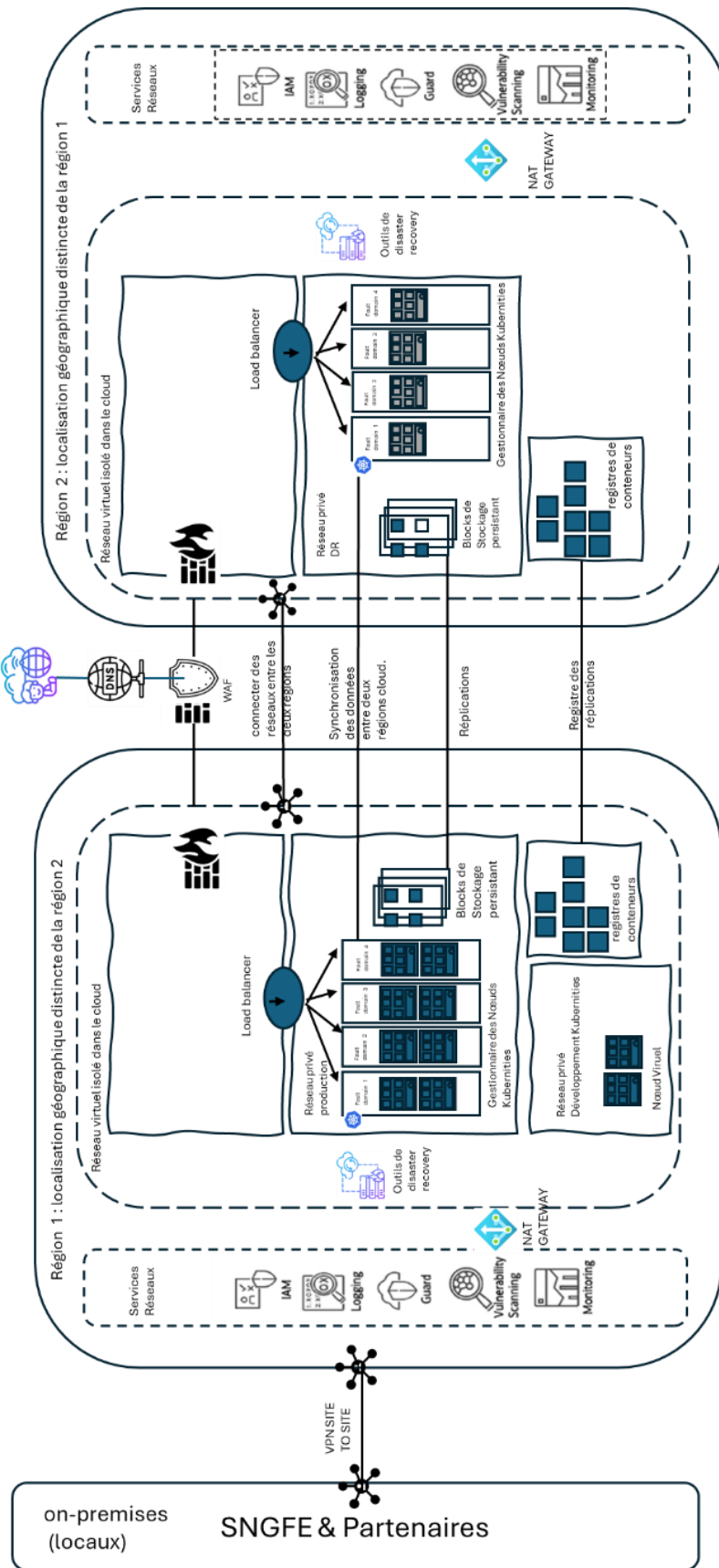
- **Kubernetes Clusters :**
 - Environnements de production et de développement distincts.
 - Support des nœuds Kubernetes sur des sous-réseaux privés pour plus de sécurité.
 - Utilisation d'un Kubernetes managé pour un provisionnement élastique des ressources.
- **Registre Docker :**
 - Réplication des images de conteneurs entre les deux régions pour garantir la disponibilité.

e. Résilience et Monitoring

- **Disaster Recovery (reprise après sinistre) :**
 - Synchronisation des volumes de stockage (Block de Stockage) entre les sites via des outils.
 - Outils automatisés d'orchestration du basculement de l'activité vers le site DR
- **Logging et Monitoring :**
 - Surveillance des performances des workloads et des clusters avec des outils.
- **Sécurité et Scans de Vulnérabilités :**
 - Protection des environnements contre les menaces et les failles de sécurité.

f. Services Complémentaires

- **Load Balancers :**
 - Distribution de charge entre les pods des applications.
- **NAT Gateway :**
 - Gestion des connexions sortantes pour les nœuds privés.
- **Stockage Objet :**
 - Stockage des journaux, des sauvegardes et des artefacts.



3. Journalisation (Logging) et monitoring :

- La solution proposée doit inclure des services de monitoring et de logging qui peuvent s'interfacer avec les outils supervision utilisés par SNGFE type Syslog et SIEM via API.
- La supervision de l'ensemble des objets de l'orchestrateur doit permettre la notification des alertes aux équipes de supervision et d'exploitation en utilisant des règles de notifications ;
- La solution retenue doit avoir une interface web pour le monitoring en temps réel, l'état de santé du cluster et des objets dépendants ;
- La solution doit intégrer une solution de Monitoring/Alerting et de Logging de tous les composants des systèmes supportés par l'éditeur.

4. Sécurité et Réseau :

Dans cette partie nous listons les critères de sécurité que doit satisfaire la solution adoptée : Le soumissionnaire est invité à présenter tous les arguments et détails techniques nécessaires, permettant d'évaluer les mécanismes de sécurité et outils de contrôle développés ci-dessous.

La solution doit inclure les fonctionnalités avancées de gestion du réseau et de la sécurité entre l'ensemble des objets de l'orchestrateur :

- Gestion de la communication réseau entre les différents objets Kubernetes
- Sécurisation des interactions entre les Pods ;
- Sécurisation des flux entre les espaces de noms (namespaces).
- Gestion des certificats SSL ;
- Possibilité d'intégration avec l'annuaire Microsoft Active directory de la SNGFE ;
- La solution doit proposer un module d'identification et de gestion des utilisateurs pouvant être fédéré (SAML 2.0) avec plusieurs solutions du marché (Microsoft AD, ...)
- L'import des groupes Active Directory dans la solution et l'affectation des rôles par groupe ;
- La solution doit permettre la mise en place de mécanismes de détection des vulnérabilités et leur remédiation.
- La plateforme doit permettre de créer une arborescence (multi-niveaux) logique des ressources (Network, Compute, ...) afin de mieux gérer les projets et les accès à ces groupes logiques.
- La plateforme doit proposer un module de Quota afin de limiter les ressources par groupe logique.
- La Solution doit proposer un module (Infrastructure as Code) pour automatiser les déploiements via du Scripting (Terraform, Ansible, ou autre).
- La solution doit permettre la mise en place d'un proxy en sorti du cluster. Les adresses IP des noeuds ne doivent pas être l'adresse IP source ;
- Intégration avec les loads balancer;
- Les permissions de la solution doivent suivre le principe zero-trust security. Toute action doit être explicitement permise.
- Contrôle et sécurité du flux EST/OUEST et NORD/SUD au sein d'une Solution Kubernetes :

La solution doit offrir les possibilités d'intervenir pour filtrage d'un flux réseau à tous les niveaux et surtout entres Endpoint . Les techniques de filtrage à prendre en charge sont :

- Par IP (N3)
- Par Port (N4)
- Par application (N7)
- Fonctionnalité WAF (Reverse Proxy) interne à la solution en vue d'assurer une communication sécurisée (EST/OUEST et NORD/SUD)
- Un protection FW applicatif (N7) : avec fonctionnalité :Vulnérabilité scanning , IPS DDOS
- Sécurité des conteneurs :
 - La solution proposée doit assurer Protection contre les vulnérabilités au niveau du noyau système et des librairies ou application abritées ;
 - La solution doit permettre l'inspection de l'activité des processus et des files systèmes dont le but de détection tout comportement suspect au sein des conteneurs.
- Chiffrement des données :
 - Les données doivent être chiffrées avec une clé cryptographique « AT REST » et « IN TRANSIT »
 - La plateforme doit permettre la gestion des Clés cryptographiques avec un Key Manager interne ou externe à la solution.
 - La plateforme doit être accessible à travers une connexion réseau sécurisée pour les utilisateurs interne de la SNGFE depuis le siège. Elle devra également être accessible à travers un VPN Client2Site ou Site2Site (ex : intégrateurs, entités partenaires, ...)

Le Titulaire est invité à compléter et à mettre en œuvre la checklist du DISA STIG, disponible à l'adresse suivante : <https://public.cyber.mil/stigs/downloads/>, relative au durcissement en matière de sécurité (hardening) de l'infrastructure cible.

- Sécurité des hôtes et cluster

A l'instar du conteneur les hôtes physiques doit être monitorée et superviser contre les risques ci-dessous :

- Elévation des privilèges
- Supervision d'usage des comptes à privilège et compte de services
- Supervision de tout changement des droits admins du cluster
- Supervision de l'arrêt des services critiques à l'infrastructure comme API Server ou Docker daemon

- Sécurité du système d'orchestration et ses ressources :

La solution d'orchestration et différents outils de management de l'orchestrateur présentent par nature une surface d'attaque à haut risque. Ainsi, il est impératif de proposer des solutions permettant d'assurer un niveau de protection acceptable.

Pour ce faire, la SNGFE exige la prise en charge des fonctionnalités ci-dessous :

- Protection et renforcement de la sécurité de l'API Server via des techniques comme RBAC, Les règles Firewall local pour une protection contre les accès et tentatives d'intrusions illégales ;

- L'accès aux API à sécuriser via des mécanisme d'authentification, Autorisation et Accounting (Tracabilité) ;
 - Les permissions du composant Kubelet doivent être les plus restrictif : usage RBAC, Rotation de certificats est souhaitable ;
 - Revue et fiabilisation pour les ports utilisés depuis l'externe et suppression des ports et services inutiles ;
 - Restreindre l'accès à la console de management au strict Minimum ;
 - La sécurité de la solution doit suivre le principe Zéro-Trust Security. Toute action doit être explicitement permise.
- Activer le volet traçabilité sur l'ensemble du périmètre (qui fait quoi comment et quand ?) ;
 - La conformité technique doit se faire sur la base CIS benchmark ou un référentiel équivalent ;
 - Les outils à fournir pour assurer la supervision et gouvernance sécurité doivent être présentés et détaillés avec des exemples et écrans tant que possible ;
 - La solution doit permettre la notification temps réel sur des risques à prédéfinir.

5. Gestion des Images :

- La solution doit inclure une Marketplace ou des images de conteneurs éditées et certifiées par l'éditeur de la solution.
- La solution doit inclure un registre pour héberger les images de conteneurs.
- La solution permet l'exposition du registre des conteneurs des images en externe.
- La solution permet de scanner, signer, et vérifier les images des conteneurs par les administrateurs afin de s'assurer de leur intégrité.

6. Gestion de Stockage et Sauvegarde

- La solution doit inclure la gestion du stockage persistant automatisé pour les différents types (Blocks, Fichiers, Objets)
- La solution doit offrir, nativement, un outil de sauvegarde des disques.
- La solution doit offrir des politiques de sauvegarde prédéfinies et aussi permettre de définir des politiques spécifiques.
- La solution doit s'intégrer avec l'outil de sauvegarde de la SNGFE (Veeam et Synology).
- La plateforme doit offrir plusieurs niveaux de stockage Objets (Standard et Archive) afin de prévoir une rétention à long terme.
- L'ensemble des configurations du cluster doivent être sauvegardés.
- La plateforme doit offrir, nativement, des mécanismes de réplication entre les différents sites.
- Le stockage persistant doit être sauvegardé.
- La solution doit permettre le test de restauration des configurations et du stockage persistant.

Le titulaire devra mettre en place la configuration et les processus en collaboration avec les administrateurs pour qu'elle puisse s'interfacer avec les solutions de sauvegarde et les solutions de supervision exemple (Zabbix).

7. Répartition de charge et haute disponibilité

La solution doit inclure un répartiteur de charge supporté par l'éditeur qui permet :

- La répartition de charge entre les différents nœuds assurant le rôle API Kubernetes.
- La répartition de charge entre les différents nœuds assurant le flux entrant http et https depuis l'extérieur vers l'orchestrateur.
- La solution doit offrir plusieurs modes de répartition de charges couvrant les niveaux OSI couches 3 et 4 (TCP/UDP/ICMP) ou bien les niveaux 4 (TCP) et 7 (HTTP).
- La solution doit garantir la haute disponibilité à tous les niveaux des composants critiques de l'orchestrateur.
- La solution doit supporter la haute disponibilité multi sites (redondance géographique).
- La solution doit offrir un niveau de disponibilité (SLA) d'au moins 99.5% attesté par l'éditeur.
- La plateforme doit permettre de faire des simulations et des tests de basculements entre le site principal et le site backup.
- La plate-forme doit être répliquée sur 2 sites, basés au Maroc et doit permettre un basculement manuel et automatique d'un site vers l'autre. Résilience : afin d'assurer un maximum de disponibilité et de haute disponibilité, la plateforme doit être déployée sur au moins 3 Fault Zones par site (Racks séparés).

8. Scalabilité de l'orchestrateur, Mises à jour et upgrade

- La solution doit permettre l'ajout et la suppression automatisée des nœuds de l'orchestrateur.
- La solution doit supporter la mise à jour et montée en version de l'orchestrateur d'une manière simple « en one click update & upgrade »
- La plateforme doit proposer automatiquement les patches et les montées en version.
- La solution doit permettre une mise à niveau des nœuds en deux modes « In-Place » ou « Out-of-place »

9. Fourniture d'une connexion à internet symétrique, et redondante (opérateurs différents), ainsi que le domaine et le certificat wildcard

Le prestataire doit fournir une bande passante ayant les caractéristiques suivantes :

- Bande Passante Internet 10 Mbps fournie sur deux (2) lignes symétriques redondantes (deux connexions Internet distinctes provenant de deux fournisseurs d'accès Internet différents) ;
- 1 (Un) service LAN2LAN qui permet de connecter des environnements on-premises (locaux) directement aux infrastructures cloud via des connexions privées, rapides et sécurisées de minimum 1GBPS
- Transfert mensuel : illimité
- 10 adresses IPv4 publiques. De plus. Le prestataire s'engage à fournir un nom de domaine et un certificat SSL Wildcard pour le nom de domaine fourni, et à assurer la gestion DNS publique pour ce domaine tout au long de l'exécution du présent marché.

10. Formation :

- Le Titulaire doit assurer la formation et un transfert de compétences par un formateur certifié pour la solution, nécessaire pour la montée en compétence des équipes projets SNGFE.
- Le Titulaire doit proposer des formations en-ligne et des certifications éditeur.

III. Mise en place de la solution

1. Cadrage, analyse du projet, Intégration et test de la solution :

La mise en place de la solution devra être exécuté dans un délai de **quinze (15) jours** à partir de la date prescrivant le commencement des prestations et ce conformément à l'article 13 du présent cahier des prescriptions spéciales. Cette prestation devra inclure les éléments suivants :

- Produire un plan d'assurance qualité du projet ;
- Produire la note de cadrage et organiser la réunion de démarrage ;
- Animer des ateliers pour convergence et cadrage du périmètre du projet ;
- Animer des ateliers d'analyse du besoin ;
- Réaliser une étude technique et architecturale de déploiement ;
- Installer la solution et mettre en place les liaisons VPN selon les prérequis techniques arrêtés lors de l'analyse technique ;
- Effectuer les paramétrages nécessaires ;
- Effectuer la reprise des données ;
- Réaliser les tests de sécurité ;
- Réaliser les tests internes et les tests recette en collaboration avec les équipes SNGFE ;
- Corriger les anomalies et stabiliser le système.

IV. Livrables:

Le Titulaire doit produire les livrables suivant pour l'Article 1 :

- Solution déployée et opérationnelle ;
- Plan de durcissement (hardening) validé avec le maître d'ouvrage, incluant les mesures de sécurité appliquées ;
- Checklist DISA STIG complétée et mise en œuvre ;
- Documentation des configurations de l'orchestrateur, des conteneurs, pods, et solutions de sécurité (pare-feu, WAF, etc.) ;
- Planning détaillé de réalisation de la mission ;
- Rapport d'analyse décrivant l'architecture technique de la solution ;
- Rapport d'installation de la solution ;
- Rapport des tests de sécurité validée et la correction des failles détectées ;
- Rapport de validation des tests recette ;
- Manuel d'utilisation de la solution paramétrée ;
- Manuel d'administration ;
- Document détaillant la procédure de gestion des logs de l'orchestrateur ;

- Document détaillant la sauvegarde et la restauration des configurations du cluster, du stockage persistant et des bases de données ;
- Document livrable pour les procédures d'exploitation de la solution.

PRIX N° 2 : Prestation d'infogérance de la solution :

Le Titulaire devra assurer la gestion, l'exploitation, l'optimisation et la sécurisation du système d'information dédié à cette opération, selon les axes suivants :

1. Administration des applications, conteneurs et pods

- Assurer les interventions de proximité sur tous les composants de la plateforme, ainsi que leur supervision continue 24/7/365 ;
- Contribuer aux analyses et proposer des axes d'amélioration et de fiabilisation, notamment en matière de protection et de sécurité (pare-feu applicatif) ;
- Implémenter la sécurité périmétrique incluant antivirus, pare-feu, WAF, VPN, protection DDoS, IPS et logging ;
- Appliquer les mesures de sécurité définies dans le plan de durcissement validé avec le maître d'ouvrage ;
- Effectuer des contrôles réguliers du WAF, détecter les vulnérabilités, surveiller les attaques virales et les menaces potentielles pour identifier tout comportement anormal ;
- Traiter les alertes de sécurité détectées.

2. Supervision et Monitoring :

- Notifier en temps réel le maître d'ouvrage en cas d'incidents détectés via l'outil de supervision liés aux conteneurs et applications publiées ;
- Vérifier régulièrement les équipements de sécurité pour identifier toute alerte ou tentative d'attaque ;
- Analyser les alertes pour distinguer les véritables menaces des faux positifs ;
- Définir, suivre et mettre en œuvre un plan de réponse aux incidents de sécurité ;
- Traiter toutes les alertes de sécurité détectées.

3. Traitement des demandes d'infogérance

Le prestataire sera chargé d'assurer les services liés à chacune des solutions suivantes :

3.1 Plateforme as a Service (PaaS)

- Création de nouveaux conteneurs ou pods, dimensionnement, configuration et gestion des actifs existants ;
- Administration et configuration du Kubernetes ;
- Assurer la mise en place des connexions demandées (Internet, LAN-to-LAN, VPN IPsec, VPN SSL, etc.).

3.2 Firewall as a Service (FWaaS)

- Paramétrage des fonctionnalités liées à la solution Firewall ;
- Mise en place et gestion du WAF pour les applications publiées.

3.3 Backup as a Service (BaaS)

- Implémenter les stratégies de sauvegarde validées par le maître d'ouvrage pour les conteneurs et pods ;
- Étendre l'espace de sauvegarde en cas de saturation contrôlée ;
- Réaliser et documenter les tests de sauvegarde et de restauration avant la mise en production ;
- Procéder à la restauration des conteneurs et pods à la demande du maître d'ouvrage ;
- Assurer la copie des sauvegardes vers des solutions de stockage objet ou des archives dédiées.

4. Livrables de la prestation d'infogérance :

4.1 Rapports réguliers

- Rapport mensuel sur les incidents : Liste détaillée des incidents survenus, leurs causes, les actions correctives, et les délais de résolution.
- Rapport mensuel d'activités de support : Synthèse des demandes traitées, du temps consacré et des résultats obtenus.
- Rapport mensuel sur la consommation de la bande passante : Analyse de l'utilisation des ressources réseau, incluant des alertes en cas d'anomalies.
- Rapport mensuel sur la consommation des ressources : Vue globale des ressources consommées par la plateforme (CPU, RAM, stockage).
- Rapport mensuel détaillé par conteneur/pod : Analyse granulaire des performances et de l'utilisation des ressources pour chaque composant.

4.2 Vérifications et tests

- Rapports de tests de sauvegarde/restauration effectués avant la mise en production.
- Résultats des contrôles réguliers du WAF, incluant les vulnérabilités détectées et corrigées.
- Rapports d'analyse des alertes de sécurité, distinguant les menaces réelles des faux positifs, et des plans de réponse aux incidents.

4.3 Assistance et mise en œuvre

- Dossier de création et de configuration des nouveaux conteneurs, pods ou connexions réseau demandées.
- Documentation des mises à jour ou ajustements des règles du pare-feu et du WAF.
- Fiches techniques des extensions ou ajustements d'espace de sauvegarde.

4.4 Copies et sauvegardes

- Copies des sauvegardes effectuées (y compris leur transfert vers des solutions de stockage objet ou des archives dédiées).
- Preuve des restaurations réalisées sur demande, incluant les étapes suivies et les délais respectés.

PRIX N° 3 : Provision d'assistance particulière :

Le Titulaire devra mettre à la disposition de la SNGFE des collaborateurs afin qu'ils assistent les différentes parties prenantes pour s'assurer de leur capacité à mettre en œuvre la solution. Cette assistance consistera en l'exploitation de la solution objet du marché.

Le prestataire devra fournir une assistance sur site ou à distance en cas de besoin et ce suivant la demande de la SNGFE.

Le prestataire doit mettre à disposition de la SNGFE en cas de besoin des ressources sur site certifiées sur la solution objets d'assistance.

Pour chaque demande, il s'agit de :

- L'assistance technique et fonctionnelle autour des technologies de la solution objet du marché ;
- La prise en charge de tout nouveau besoin demandé par la SNGFE ;
- Missions d'assistance et de conseil (nouvelles architectures, nouvelles implémentations, ...) ;
- La veille technologique ;
- Audit, Tuning, & divers intervention ;
- Implémentation des nouvelles fonctionnalités et mise en place des configurations permettant l'amélioration des performances, de l'administration et l'exploitation, la sécurité, la disponibilité et la continuité d'activité.

Les livrables de cet article seront définis dans la demande d'assistance formulée par le maître d'ouvrage.

Article 28 : Autres dispositions

1. Accord de niveau de SLA

1.1 Garantie de temps de rétablissement du service (GTR)

Le titulaire s'engage sur la disponibilité du service de la plateforme 24h/24h et 7 jours/7 et à fournir un numéro de contact d'urgence.

Le service sera considéré indisponible en cas d'impossibilité pour le maître d'ouvrage d'accéder via internet ou VPN à l'une des composantes de la plateforme ou à ses services, sous réserve que cette indisponibilité résulte d'un fait exclusivement imputable au titulaire ou à ses fournisseurs.

Le titulaire s'engage sur un temps de rétablissement du service de deux (02) heure à partir de la notification par le maître d'ouvrage de l'indisponibilité du service.

Le Temps de rétablissement du Service s'étend entre l'ouverture d'un ticket d'incident et sa résolution. Le ticket est créé par le titulaire à compter de la réception de la notification de l'incident de la part du maître d'ouvrage et ce, par tout moyen de communication (courriel, portail helpdesk ou téléphone) lui notifiant l'indisponibilité du Service. Toutefois, pour des fins de traçabilité, l'usage de l'email et du portail helpdesk doivent être privilégiés. Un accusé de réception d'ouverture du Ticket est envoyé automatiquement par e-mail au maître d'ouvrage, détaillant les anomalies constatées.

Une demande exprimée par le Maître d'ouvrage est considérée comme incident et subit le même traitement du GTR.

Le Ticket est affecté à l'équipe technique du Titulaire dédié au présent marché qui se chargera de résoudre la demande du maître d'ouvrage. Le Ticket est clôturé lorsque l'anomalie a été traitée.

A la fin de chaque mois, les durées des éventuelles indisponibilités de service sur la période écoulée sont comptabilisées par le Titulaire et le Maître d'Ouvrage.

1.2 Garantie du temps de mise en conformité (TMC)

À tout moment, le maître d'ouvrage peut vérifier la conformité de la configuration demandée, en utilisant les deux méthodes de vérifications suivantes :

Vérifications sur les lieux dont le titulaire est tenu de faciliter l'accès.

Vérifications à travers les connexions à distance.

La non-conformité d'une partie ou plus de la configuration demandée est considérée comme incident et subit le même traitement du GTR.

2. Souveraineté sur les données

Le titulaire s'engage à héberger les données du maître d'ouvrage au niveau du territoire national (Maroc) et que les données restent sous la juridiction de la loi Marocaine conformément à la Directive Nationale de la Sécurité des Systèmes d'information (DNSSI).

3. Audit et Réversibilité

Pendant toute la durée du marché, le Maître d'Ouvrage est en droit d'auditer ou de faire auditer la plateforme cible. Ces audits porteront sur le respect des niveaux de service / (3/w/16 Bkam) et la sécurité du Centre de Traitement des Données du titulaire. Ces audits sont réalisés par l'équipe du Maître d'ouvrage ou par un Prestataire de son choix

En conformité avec les exigences de la loi n° 05-20 relative à la gestion des services publics, le titulaire du marché s'engage à garantir la réversibilité des services fournis à l'issue du marché. À la fin de la période de prestation, ou en cas de résiliation anticipée du marché, le prestataire devra procéder, sans délai et à ses frais, au transfert intégral des actifs, données, équipements, logiciels et autres ressources nécessaires à la continuité du service, dans les conditions définies par le présent cahier des charges. Ce transfert devra être effectué de manière transparente et dans un environnement sécurisé, avec la collaboration des parties prenantes, afin de garantir une transition fluide vers le nouveau gestionnaire ou l'entité publique concernée. Le prestataire devra également fournir un accompagnement technique et former le personnel nécessaire pour assurer la continuité des opérations, conformément aux normes de qualité et aux engagements de service définis dans le marché.

4. Respect des référentiels et lois relatifs à la sécurité des Systèmes d'information

Le titulaire doit obligatoirement respecter les mesures et les recommandations figurant dans la DNSSI, Décret n° 2-24-921 DGSSI, la Dir 4/w/2022 et la loi 05-20 relative à la cybersécurité.

5. Accès aux données

Le titulaire doit permettre au maître d'ouvrage un accès sécurisé à la plateforme 24/24 7j/7 durant toute la période du marché

6. Résilience et sécurité du site

Dans le cadre de ses prestations, le Prestataire assure, conformément aux règles de l'art et des standards internationaux en vigueur en la matière, la sécurité du site où sont hébergées les infrastructures objets du marché. Le système de sécurité et de résilience, assuré par le Prestataire, comprend les éléments suivants :

- L'ensemble du site (l'intérieur et l'extérieur du bâtiment), doit être placé sous vidéo surveillance et télésurveillance constante 24h/24h - 7j/7j, en temps réel ;
- Un système électrique performant et redondante, ainsi qu'un système palliatif d'un éventuel arrêt du réseau électrique, avec, entre autres, une distribution électrique doublée, une énergie primaire doublée (onduleur, groupe électrogène...) ;
- Un système thermique et hygrométrique répondant aux attentes du Client (redondance des unités de climatisation, capacité de refroidissement. . .) :
- Un système de détection des inondations ;
- Un système de détection et de lutte contre l'incendie. La maintenance de ces systèmes est assurée par le Prestataire. À l'égard à la nature des Prestations, le Prestataire garantit avoir mis en place des conditions de sécurité optimales en vue d'interdire et prévenir tout accès physique de personnes non autorisées aux Matériels du Client hébergé sur son Site de Production.

A ce titre, le Prestataire assure :

- Le suivi de la sécurité ;
- La mise en place de système de détection d'intrusion :
 - La remontée des alertes ;
 - Le contrôle d'accès aux sites. Le contrôle d'accès au Site de Production s'effectue à l'entrée et à la forme d'une vérification de l'identité des personnes.

6.1 Règles de sécurité

Le Titulaire et son personnel sont tenus de respecter toutes les dispositions législatives ou réglementaires de sécurité, les règles de sécurité internes du Maître d'Ouvrage et les bonnes pratiques en la matière. Dans ce sens, le Titulaire et son personnel sont tenus de respecter, entre autres, les règles de conduites générales suivantes :

- Ne pas manipuler les installations techniques et équipements sans autorisation du Maître d'Ouvrage ;
- Les intervenants mandatés par le Titulaire doivent se limiter uniquement au périmètre précis de leurs interventions objet du marché (local, matériel, équipements) : Ils ne doivent en aucun cas accéder aux locaux, matériel ou équipements non inclus dans leurs interventions ;
- S'interdire de prendre des copies des documents et des supports d'information qui lui/leur sont confiés, à l'exception de celles qui sont nécessaires à l'exécution des prestations prévues dans le cadre du présent marché. L'accord préalable du maître d'ouvrage étant obligatoire ;
- Prendre toutes les mesures permettant d'éviter toute utilisation détournée ou frauduleuse des données traitées au cours de l'exécution du présent marché ;
- Prendre toutes les mesures de sécurité pour assurer la conservation et l'intégrité des documents et informations traités pendant la durée du présent marché ;
- Procéder, à la fin du marché, à la destruction de tout fichier ou document dont il dispose, quel qu'en soit le support, et qui stockerait des informations propres au maître d'ouvrage ;

- Respecter les exigences de sécurité dictées par la politique de sécurité du système d'information adoptée par le maître d'ouvrage.
- Respecter les exigences de sécurité dictées par la charte d'utilisation du système d'information du maître d'ouvrage. Le Titulaire est tenu d'informer son personnel des dispositions de sécurité et des règles de conduite du Maître d'ouvrage. Tout le personnel du Titulaire ou de ces éventuels sous-traitants devant intervenir dans l'exécution du marché est tenu de respecter desdites règles de sécurité.

6.2 Vérification des règles de sécurité

Le Maître d'Ouvrage se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect du Titulaire des obligations précitées par le maître d'ouvrage. Les obligations de confidentialité et de sécurité doivent être respectées durant toute la durée d'exécution du présent marché. Elles persisteront même après l'exécution du marché et resteront en vigueur tant que les informations et documents confidentiels ne sont pas passés dans le domaine public.

7. Obligation et responsabilité du titulaire

Au titre de l'exécution du marché, le Prestataire s'engage à fournir les prestations conformément aux niveaux de disponibilité, de continuité et de qualité de service définies au présent marché. Il est tenu à une obligation de moyens à l'égard de la technicité des technologies mises en œuvre. Le titulaire exécutera les prestations, objet du présent marché, en conformité avec les règles de l'art de sa profession concernant les techniques et méthodes utilisées. Il s'engage à fournir tous les soins nécessaires pour la bonne exécution du marché, en étroite collaboration avec le maître d'ouvrage et s'engage à réaliser, aux conditions acceptées par les deux parties, les prestations demandées par le maître d'ouvrage.

Le titulaire s'engage à respecter les différentes contraintes et obligations suivantes :

- La Haute Disponibilité : le titulaire s'engage à maintenir les temps d'indisponibilité des systèmes et services déployés au niveau de la plateforme à un minimum, avec un taux de disponibilité garanti égal ou supérieur à 99,5%.
- La Sécurité : La plateforme proposée devra assurer l'intégrité et la confidentialité nécessaires aux systèmes d'information du Maître d'Ouvrage. Le titulaire doit ainsi prendre toutes les mesures nécessaires pour anticiper et contrer toute menace potentielle d'interception, de modification ou d'interruption des systèmes déployés.

Le titulaire du marché est tenu également de :

- Réaliser les prestations et installations conformément aux normes et à la réglementation en vigueur en utilisant et les éditions compatibles les plus récentes ;
- Garantir la protection et la confidentialité des données hébergées en s'abstenant d'agir sur les données hébergées, sauf en cas de demande expresse du maître d'ouvrage ;
- Conseiller, assister et mettre en garde le maître d'ouvrage conformément aux dispositions du présent marché et dans un esprit de loyauté et de bonne foi ;
- Mettre en place les moyens humains et matériels pour assurer une exécution satisfaisante du marché ;

- Informer préalablement le maître d'ouvrage des horaires des interventions éventuelles sur la plateforme ;
- Donner à son personnel les instructions nécessaires et leur prescrire les consignes à suivre pour assurer la protection des données, des systèmes et des services du maître d'ouvrage.

Article 29: Décomposition du montant global

DECOMPOSITION DU MONTANT GLOBAL

N° prix	Désignation des prestations	Unité de mesure	Quantité	Prix unitaire en Dirhams (hors TVA)		Prix total
				En chiffres	En lettres	En chiffres
1	Services d'hébergement et d'orchestration managés de conteneurs, incluant la gestion des charges de travail (workloads) et l'automatisation des déploiements au profit de la SNGFE	Forfait	1			
2	Prestation d'infogérance de la solution	Forfait	1			
3	Provision d'assistance particulière	J/H	10			
TOTAL HT						
TVA (20%)						
TOTAL TTC						

Arrêté le présent bordereau à la somme de : ... dirhams Toutes Taxes Comprises (... DH T.T.C)

Maché n° .../2024/SNGFE

OBJET : Hébergement et orchestration managés de conteneurs incluant la gestion des charges de travail (workloads) et l'automatisation des déploiements au profit de la Société Nationale de Garantie et du Financement de l'Entreprise

pour un montant annuel de (en chiffres et en lettres) :
.....
.....

Lu et Accepté Par :
(Titulaire)

Approuvé Par :

Directeur Général Adjoint Ressources

Signé : Abdeikhalek GLILLAH