REPUBLIQUE DE GUINEE

Travail-Justice-Solidarité

……

MINISTERE DES POSTES, DES TELECOMMUNICATIONS ET DE L'ECONOMIE NUMERIQUE (MPTEN)

……..

PROJET DE TRANSFORMATION NUMERIQUE POUR L'AFRIQUE/PROJET REGIONAL D'INTEGRATION NUMERIQUE EN AFRIQUE DE L'OUEST (WARDIP-GUINEE)

AVIS A MANIFESTATIONS D'INTERET

SERVICES DE CONSULTANT (Individu)

Client : Ministère des Postes, des Télécommunications et de l'Economie Numérique (MPTEN) représenté par le Projet Régional d'Intégration Numérique en Afrique de l'Ouest (WARDIP-GUINEE).

Référence de l'accord de financement : IDA : Crédit N° 74440GN

L'APPEL A MANIFESTATION D'INTERET POUR LE RECRUTEMENT D'UN(e) CONSULTANT(e) RESEAUX ET SECURITE SENIOR

Date début : 19 mai 2025 **Date limité : 16 Juin 2025**

Contexte et justification de la mission

Le Gouvernement de la République de Guinée a obtenu un financement de 60 millions de dollars $ de l'Association Internationale pour le Développement (IDA) pour financer le coût du Projet de Transformation Numérique pour l'Afrique/ Projet Régional d'Intégration Numérique de l'Afrique de l'Ouest (DTfA/WARDIP) placé sous la tutelle du Ministère des Postes, des Télécommunications et de l'Economie Numérique (MPTEN). Le Projet a l'intention d'utiliser une partie de ce montant pour effectuer les payements au titre du **Recrutement d'un (e) consultant (e) réseaux et sécurité senior.**

Objectif de la mission :

L'objectif est de recruter un(e) ingénieur(e) réseaux et sécurité afin de concevoir, mettre en œuvre, maintenir et sécuriser l'infrastructures réseau des services publics numériques.

MISSION DU CONSULTANT

Sous l'autorité directe du chef de projet et en étroite coordination avec l'équipe projet, le/la consultant(e) ingénieur(e) réseaux et sécurité aura pour responsabilité majeure de garantir la fiabilité, l'intégrité, la disponibilité et la sécurité permanente des infrastructures réseau et des systèmes d'information des services publics numériques.

Principales responsabilités :

Conception et déploiement d'infrastructures réseau sécurisées :

- Concevoir et implémenter des architectures réseau robustes, évolutives, performantes et sécurisées conformément aux meilleures pratiques internationales (ISO 27001, NIST, CIS Controls) ;
- Installer, configurer et optimiser les équipements réseau critiques (switches, routeurs, pares-feux, load balancers, systèmes sans-fil sécurisés, etc.).

Documentation technique détaillée :

- Élaborer et maintenir à jour les schémas d'architecture réseau, topologies détaillées et documentations techniques exhaustives.

Configuration avancée et gestion proactive des services réseau :

- Déployer et administrer les protocoles et services essentiels : DNS sécurisé (DNSSEC), DHCP sécurisé, VLAN, VPN/IPSec, etc ;
- Gérer les mises à jour logicielles, les patchs de sécurité et les migrations techniques, minimisant l'impact sur les utilisateurs finaux.

Surveillance continue et gestion opérationnelle :

- Mettre en œuvre des outils de monitoring réseau performants (Nagios, Zabbix, PRTG, ou équivalents) et produire des tableaux de bord proactifs ;
- Assurer la surveillance permanente de l'infrastructure réseau et intervenir rapidement pour diagnostiquer, analyser et résoudre les incidents techniques ou de sécurité.

Sécurité avancée et gestion des incidents :

- Concevoir et appliquer rigoureusement les politiques de sécurité réseau (firewalls avancés, IDS/IPS, filtrage web, antivirus, antimalware) ;
- Réaliser périodiquement des audits de sécurité, des tests d'intrusion et des évaluations approfondies des vulnérabilités ;
- Mettre en place des processus de réponse rapide aux incidents de sécurité, y compris l'investigation numérique et la remédiation efficace.

Gestion de la continuité opérationnelle (PCA/PRA) :

- Élaborer et déployer des stratégies rigoureuses de sauvegarde, reprise après sinistre et de continuité d'activité, en adéquation avec les exigences du secteur public.

Veille proactive en sécurité et innovation technologique :

- Réaliser une veille continue sur les nouvelles technologies, les menaces émergentes, les réglementations en vigueur et les meilleures pratiques en cybersécurité ;
- Proposer des améliorations technologiques et méthodologiques régulières pour anticiper et réduire les risques.

Support technique et renforcement des capacités internes :

- Fournir un support technique spécialisé et réactif aux utilisateurs internes en cas d'incidents réseau.
- Organiser et animer des formations régulières destinées aux utilisateurs pour renforcer leurs compétences et sensibiliser aux bonnes pratiques de sécurité informatique.

Reporting et gouvernance efficace :

- Préparer des rapports d'avancement détaillés à l'attention du chef de projet, incluant indicateurs de performance, incidents notables et recommandations d'amélioration ;
- Participer activement aux réunions d'équipe et assurer une communication fluide et efficace avec l'ensemble des parties prenantes.

Collaboration et autres tâches :

- Assurer une étroite collaboration transversale avec les autres membres de l'équipe projet (architectes, développeurs, gestionnaires de projet) et toutes autres parties prenantes impliquées ;
- Toute autre tâche ou mission complémentaire définie par le chef de projet ou exigée par l'évolution du projet.

Le Ministère des Postes, des Télécommunications et de l'Economie Numérique (MPTEN) représenté par le Projet de Développement de l'Agriculture Commerciale en Guinée (WARDIP-GN) invite les Consultants individuels à présenter leur candidature en **langue française** en vue de fournir les services décrits ci-dessus. Les consultants intéressés doivent fournir les documents

suivants : Cv, lettre de motivation, références, diplômes, attestations de services faits et attestations de formations complémentaires.

PROFIL DU CONSULTANT

Le/la consultant(e) recherché(e) doit faire preuve d'une excellente capacité à évoluer dans un environnement multiculturel complexe et à gérer efficacement des relations professionnelles avec divers interlocuteurs (institutions gouvernementales, agences publiques, entreprises privées et autres partenaires techniques). Il/elle doit démontrer une solide expérience dans la conception, la gestion et la sécurisation d'infrastructures réseau complexes et des systèmes d'information critiques, idéalement dans un contexte public ou institutionnel.

Le/la candidat(e) idéal(e) doit disposer d'une forte capacité analytique, faire preuve d'autonomie et d'initiative dans la résolution proactive de problèmes complexes. Il/elle doit démontrer un engagement fort pour la veille technologique permanente, le partage des connaissances et la diffusion des bonnes pratiques auprès des équipes internes.

Les critères pour l'évaluation des candidatures seront :

- **Formation académique :**
    - Diplôme d'ingénieur ou Master (Bac+5 minimum) en Informatique, Réseaux et Télécommunications, Cybersécurité, Systèmes d'information ou domaine connexe.

Absence de diplôme, diplôme non conforme ou de niveau inférieur : Disqualifié.

- **Expérience professionnelle requise :**
    - Expérience professionnelle confirmée d'au moins dix (10) ans dans le domaine de l'architecture et la sécurisation des réseaux et systèmes d'information ;
    - Au moins trois (3) missions significatives en tant qu'architecte réseaux et sécurité, incluant idéalement des projets de grande ampleur (réseaux gouvernementaux, infrastructures critiques, etc.).
- **Compétences techniques requises :**
    - Excellente maîtrise des technologies réseau fondamentales (protocoles TCP/IP, routage avancé, commutation VLAN, VPN, etc.) et équipements associés (Cisco, Fortinet, Palo Alto, ou similaires) ;
    - Expertise confirmée sur les systèmes d'exploitation courants (Linux et Windows Server) ;
    - Solide expérience pratique en cybersécurité (pares-feux avancés, IDS/IPS, SIEM, cryptographie, sécurité des applications et des systèmes, etc.) ;
    - Expérience confirmée dans la mise en place et la gestion sécurisée d'infrastructures cloud (AWS, Azure, Google Cloud ou équivalent) ;
    - Expérience avérée avec les systèmes de gestion de version (Git).
- **Compétences complémentaires fortement appréciées :**
    - Familiarité avec les pratiques DevOps et outils associés d'intégration et déploiement continu (CI/CD) : Jenkins, GitLab CI, Azure DevOps, etc ;
    - Expérience pratique en virtualisation et containerisation : VMware, Hyper-V, Docker, Kubernetes ;
    - Maîtrise d'au moins un langage de scripting ou d'automatisation : Python, Shell/Bash.
- **Certification et formation continue :**
    - Certifications reconnues en réseaux et sécurité fortement appréciées (CCNA, CCNP, CISSP, CISM, CEH, Google Cybersecurity Certificate, ou équivalents).

- Bonne connaissance des méthodes agiles (Scrum, Kanban) serait un atout supplémentaire.

- **Langues :**
  - Français (niveau maitrise) et Anglais (niveau intermédiaire à l'écrit et à l'oral).

NB : Les références doivent être accompagnées de certificats de services rendus délivrés par les bénéficiaires des prestations et indiquant la description du projet, l'étendue et la valeur du marché. En l'absence de ces documents l'expérience déclarée ne sera pas considérée.

Les critères d'éligibilité, l'établissement de la liste restreinte et la procédure de sélection seront conformes aux directives de sélection de consultants individuels de la Banque mondiale « Règlements pour la Passation des Marchés pour les Emprunteurs sollicitant le FPI » de la Banque mondiale édition septembre 2023.

Les candidats intéressés peuvent obtenir des informations supplémentaires au sujet des documents de référence (TDR) à l'adresse mentionnée ci-dessous et aux heures suivantes :

Du lundi au jeudi : de 9 heures à 16 heures 30 mn Le vendredi : de 9 heures à 13 heures.

Les expressions d'intérêt doivent être déposées ou transmises par courriel à l'adresse mentionnée ci-dessous au plus tard le **16 Juin 2025 à 12 h 00 mn GMT.** Les enveloppes doivent porter expressément la mention ***« Manifestation d'intérêt pour le Recrutement d'un (e) consultant (e) réseaux et sécurité senior ».***

À l'attention de : Monsieur le Coordonnateur par intérim du Projet Régional d'Intégration Numérique en Afrique de l'Ouest (WARDIP-GN).

L'adresse dont il est fait mention ci-dessus est : Projet Régional d'Intégration Numérique en Afrique de l'Ouest (WARDIP-GN), Quartier Kaporo, Commune de Ratoma-Conakry, Immeuble BAH Kadiatou, référence la Société Easycom et à proximité du pont Kiridi, **E-mail : coordonnateur@wardip.gn / bounawardip24@gmail.com avec copie obligatoire à : fofanafodsaidou86@gmail.com**

Fait à Conakry, le 16 mai 2025

M. Fodé YOULA
Coordonnateur par intérim de WARDIP