RÉPUBLIQUE DU BURUNDI

MINISTERE DE LA COMMUNICATION, DES TECHNOLOGIES DE L'INFORMATION ET DES MEDIAS

PROJET D'APPUI AUX FONDATIONS DE L'ECONOMIE NUMERIQUE AU BURUNDI « PAFEN »

Nº Projet : P176396/P180987

Financement : IDA : E0930-BI/E2820-BI

TERMES DE REFERENCE

POUR LE RECRUTEMENT D'UN CONSULTANT CHARGE DE LA SECURITE DU RESEAU INFORMATIQUE DE BURUNDI EDUCATION AND RESEARCH NETWORK – BERNET

MARS 2024

I. INTRODUCTION

Le Gouvernement du Burundi a obtenu un don de la Banque Mondiale pour financer le Projet d'Appui aux Fondations de l'Economie Numérique (PAFEN) en sigle (le Projet) ou « Burundi Digital Foundations Project » en anglais. Il est prévu qu'une partie des ressources de ce projet soit utilisée pour financer des prestations d'un **Consultant Informaticien Expert Sécurité Informatique** en faveur de « **Burundi Education and Research Network- BERNet** » .

II. CONTEXTE ET JUSTIFICATION

1. Objectif du Projet PAFEN

L'Objectif de Développement du Projet d'Appui aux Fondations de l'Economie Numérique (PAFEN) est d'**Accroître l'accès à l'Internet haut débit, en particulier pour les communautés mal desservies, et améliorer la capacité du gouvernement à *gérer les ressources plus efficacement et* fournir des services publics par voie numérique.**

Le projet vise à accroître l'accès au haut débit et à améliorer la capacité du gouvernement à fournir des services publics numériques, ce qui contribuera à jeter les bases d'un développement accéléré de l'économie numérique du Burundi.

Le Projet PAFEN comprend 4 composantes ci-après :

Composante 1 : Accès et inclusion numériques

- **Sous-composante 1.1** : Environnement favorable au développement du marché du haut débit et à l'accès numérique
- **Sous-composante 1.2** : Accès à la connectivité locale
- **Sous-composante 1.3** : Facilitateurs d'accès local et d'inclusion numérique

Composante 2 : Facilitateurs de la prestation de services publics numériques

- **Sous-composante 2.1** : Cadres institutionnels, juridiques, de gouvernance et technologiques pour les services en ligne
- **Sous-composante 2.2** : Infrastructure et plates-formes gouvernementales numériques partagées
- **Sous-composante 2.3** : Numérisation de certains services et de cas d'utilisation phares
- **Sous-composante 2.4** : **Modernisation des processus clés de GFP**

Composante 3 : Coordination institutionnelle et gestion du projet.

Composante 4 : Composante de réponse d'urgence (CERC).

Cette mission, s'inscrit dans le cadre de la mise en œuvre de la composante 1 du projet et particulièrement de la **sous-composante connectivité**.

2. Des Missions et Objectifs de BERNET

Burundi Education ans Research Network (BERNET) a été mis en place dans le cadre de la mise en œuvre du Projet Régional d'Infrastructure II (RCIP2) financé par la Banque Mondiale et réalisé durant la période 2008 – 2015 par le Secrétariat Exécutif des Technologies de l'information et de la Communication (SETIC).

La création de BERNET en tant qu'entité juridique au Burundi fut réalisée à l'issue des études appropriées pour développer un modèle d'entreprise viable pour assurer la durabilité à long terme du réseau et définir la structure de gestion appropriée.

Ainsi, les membres potentiels de BERNET comprennent :

- Universités publiques et privées ;
- Ecoles polytechniques publiques et privées ;
- Institutions de recherche (par exemple, santé, éducation, agriculture, minéraux, météorologie, énergie, sociologie, culture) ;
- Les bibliothèques et musées qui promeuvent et conduisent la recherche ;
- Les institutions à but non lucratif qui mènent ou promeuvent l'éducation ou la recherche, ou qui fournissent des services académiques aux institutions mentionnées ci-dessus.

Dans sa conception initiale qui reste d'actualité, du reste, BERNET avait comme principales vocations d'interconnecter, par les moyens les plus récents, les établissements d'enseignement supérieur (EES) et instituts de recherche, les unités de recherche avec quelques membres du personnel aux grandes universités nationales avec des dizaines de milliers d'étudiants et de membres du personnel académique et de leur fournir une connectivité interne et externe.

Les objectifs spécifiques de BERNET incluent :

- **La Connectivité**
  - Établir l'interconnectivité et fournir un accès à Internet pour les EES et les instituts de recherche ;
  - Fournir des services haut débit qui sont économiquement, technologiquement et institutionnellement durables.
- **L'Intégration avec les réseaux universitaires et de recherche mondiaux :**
  - Établir des partenariats et des accords de peering avec d'autres réseaux nationaux et régionaux de recherche et d'éducation en Afrique, en Europe, en Asie et dans les Amériques (par exemple l'UbuntuNet Alliance, Géant, Internet2) ;
  - Promouvoir la collaboration en matière d'éducation et de recherche aux niveaux régional et mondial.
- **La Collaboration et partage des connaissances :**
  - Établir des mécanismes pour soutenir la promotion, la diffusion et le transfert des connaissances et des technologies ;
  - Mettre en place une plate-forme de gestion des connaissances et d'échange de bonnes pratiques et d'innovations ;

- Promouvoir la collaboration par le biais de partenariats de recherche et de réseautage avec le secteur privé.

➢ **Les Services partagés :**

- Établir une plate-forme pour la construction et la prestation de services partagés pour les EES et les instituts de recherche ;
- Fournir un support ICT et une assistance technique aux membres de BERNET.

Lors de la première phase, BERNET a permis d'interconnecter autour de quinze (15) institutions de Bujumbura et de l'intérieur du pays via un réseau fibre/sans fil et/ou de un lignes louées et de fournir de la capacité internet et de transmission auxdites institutions connectées.

La deuxième phase se concentrera sur l'extension de BERNET aux autres institutions n'ayant pas été prises en charge par la phase initiale et d'améliorer les services offerts par l'association à ses membres et à la communauté.

III. MISSION DU CONSULTANT

Sous la supervision du Secrétaire Exécutif de BERNET, le consultant expert recherché sera amené à exécuter, et sans s'y limiter, les tâches suivantes :

Évaluation complète de la cybersécurité

- Effectuer une évaluation approfondie de la posture actuelle de cybersécurité de BERNET, y compris son infrastructure, ses systèmes et ses processus
- Identifier les vulnérabilités, les lacunes et les risques potentiels en matière de sécurité qui pourraient compromettre la confidentialité, l'intégrité et la disponibilité du réseau, des données et des actifs de BERNET.
- Évaluer l'efficacité des contrôles, des politiques et des procédures de sécurité actuelles dans la mitigation des risques de cybersécurité

Développement des politiques et des procédures

- Élaborer des politiques, des procédures de cybersécurité adaptées aux besoins, aux objectifs et aux exigences réglementaires spécifiques de BERNET.
- Définir clairement les rôles et les responsabilités pour la gestion de la cybersécurité, la réponse aux incidents et la conformité au sein de la structure organisationnelle de BERNET.
- Assurer l'alignement des politiques de cybersécurité sur les normes de l'industrie, les meilleures pratiques et les cadres réglementaires pertinents pour le secteur de l'éducation et de la recherche.
- Produire des rapports hebdomadaires, mensuels, trimestriels et annuels des activités ;
- Participer à l'élaboration des marchés et des contrats de fourniture d'internet.

Mise en œuvre des mesures et outils de sécurité :

- Recommander et déployer des outils, des technologies et des solutions de cybersécurité appropriés pour renforcer la posture de sécurité de BERNET.

- Mettre en place des mesures de sécurité réseau, telles que des firewalls, des systèmes de détection/prévention d'intrusion (IDS/IPS) et des solutions de sécurité des points d'accès pour protéger contre les menaces externes et internes.
- Configurer et gérer des systèmes de monitorage pour détecter et répondre aux incidents de sécurité en temps réel.

Planification de la réponse aux incidents

- Développer et documenter un plan complet de réponse aux incidents décrivant les procédures d'identification, d'évaluation et de réponse aux incidents de cybersécurité.
- Établir des protocoles de communication et des procédures d'escalade pour assurer le reporting et la coordination en temps opportun des efforts de réponse aux incidents.
- Effectuer des exercices et des simulations de table pour tester l'efficacité du plan de réponse aux incidents et améliorer la préparation organisationnelle à gérer les incidents de sécurité.

Programmes de formation et de sensibilisation

- Concevoir et dispenser des programmes de formation et de sensibilisation à la cybersécurité pour le personnel, les membres et les parties prenantes de BERNET afin de promouvoir une culture de sensibilisation et de conformité en matière de sécurité.
- Fournir des sessions de formation ciblées pour le personnel informatique et les administrateurs sur la mise en œuvre et le maintien de pratiques et de configurations informatiques sécurisées.

Monitorage et gestion des risques continue

- Mettre en place des mécanismes de monitorage continue pour détecter et répondre aux menaces, vulnérabilités et problèmes de conformité émergents en matière de sécurité.
- Mettre en œuvre des mesures de gestion des risques, telles que la numérisation des vulnérabilités, les tests de pénétration et les évaluations de sécurité, pour identifier et résoudre les faiblesses de sécurité potentielles.
- Suivre l'évolution de la réglementation et des standards de l'industrie pour garantir la conformité continue aux normes de cybersécurité pertinentes, aux réglementations et aux meilleures pratiques.

Collaboration et engagement des parties prenantes

- Collaborer avec les membres de BERNET, les organismes gouvernementaux, les partenaires industriels et les organisations de cybersécurité pour partager des informations sur les menaces, les meilleures pratiques et les ressources.
- Participer à des forums, des groupes de travail et des conférences sur la cybersécurité pour rester informé des dernières tendances, technologies et menaces en matière de cybersécurité.
- Favoriser une culture de collaboration et de partage d'informations entre les parties prenantes de BERNET

IV. PROFIL DU CANDIDAT

Le consultant devra avoir la qualification, les compétences et une expérience minimales suivantes :

- Etre détenteur d'un Diplôme de niveau Bac +4 au minimum en Informatique option sécurité des systèmes informatiques et réseaux, Génie Informatique ou Télécommunication ;
- Avoir une expérience d'au moins huit(8 ans comme Administrateur de systèmes informatiques ou de réseaux Informatiques étendus et pluri-institutionnels, Responsable de la sécurité des systèmes informatiques ;
- Posséder des certifications pertinentes telles que Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), ou équivalent. Certifications supplémentaires telles que Certified Information Systems Auditor (CISA), Certified Cloud Security Professional (CCSP), ou Expert en sécurité GIAC (GSE) serait un atout ;Maîtriser des normes et procédures de la sécurité et des outils et technologies qui s'y rapportent : firewall, end point Security, cryptographie, serveurs d'authentification, détection d'intrusion, PKI, filtrages des URL, … ;
- Avoir une bonne connaissance du matériel informatique, des protocoles internet et des réseaux ;
- Avoir une bonne maitrise des réseaux informatiques et
- Avoir une bonne maîtrise de l'administration de systèmes sous Unix, Linux, Windows, … ;
- Avoir une bonne maitrise de l'administration d'un système de virtualisation ;
- Avoir une bonne connaissance de l'administration de systèmes Cisco, BGP, OSPF… ;
- Connaissance approfondie des réseaux (communication, câblage, routeur…) ;
- Avoir une bonne maîtrise de l'utilisation des outils de surveillance réseaux, des systèmes informatiques et détection des intrusions ;
- Avoir la maîtrise des outils de suivi de projets serait un atout;
- Etre capable de travailler sous pression et de gérer le stress ;
- Avoir la maîtrise du français et de l'anglais (Ecrit et Parler);

V. DUREE DE LA MISSION

Le démarrage de la mission est prévu au début du mois de Mai 2024. La durée des prestations est d'une année renouvelable, après évaluation satisfaisante.

VI. CRITERES DE PERFORMANCE

L'efficacité et les performances de l'expert en Sécurité Informatique de BERNET seront mesurées **en fonction de son apport effectif sur la sécurisation du réseau informatique de BERNET**.

VII. CONSTITUTION DU DOSSIER

Les candidats intéressés devront fournir un dossier composé de :

- ✓ Une lettre de motivation ;
- ✓ Un curriculum vitae ;

En cas de nécessité, des copies certifiées conformes à l'original des diplômes, certificats et tout autre document attestant l'expérience professionnelle pourraient être demandés.

VIII. CONDITIONS D'EMPLOI

L'expert spécialiste en Sécurité Informatique sera un Consultant individuel rattaché à l'équipe technique de Burundi Education and Research Network (BERNET) ;

- C'est un poste de Consultant individuel à temps plein. Il sera amené à travailler dans les locaux de BERNET ;
- Le Consultant individuel est appelé à s'abstenir de toute situation qui pourrait le mettre en conflits d'intérêts dans le cadre de la mission qui lui est assignée.

IX. REMUNERATION ET ECHEANCES DE PAIEMENT

Les termes de rémunération dépendront de l'expérience et des qualifications requises conformément à la grille de l'Ordonnance Ministérielle N° 540/16667 du 24/11/2020 portant harmonisation des rémunérations et les frais de fonctionnement des gestionnaires des projets financés par les Partenaires Techniques et Financiers (PTFs).

X. METHODE ET PROCEDURE DE SELECTION

Le Consultant sera sélectionné selon la méthode de Sélection des Consultants Individuels, conformément au Règlement de Passation des Marchés pour les Emprunteurs sollicitant le financement de Projets d'Investissement (FPI), édition de Septembre 2023 et conformément aux critères exigés au regard des présents termes de référence».

La sélection de l'expert spécialiste en Sécurité Informatiques sera effectuée par appel à candidatures.

La procédure de sélection comportera deux (2) phases :

(a) Phase de présélection des candidats sur la base de comparaison des CVs des candidats sur 100 points

Cette étape sera constituée d'une présélection sur base de dossiers où seront retenus les candidats ayant les qualifications et l'expérience requises pour le poste conformément aux TdR ci-dessus.

La répartition des notes pour cette phase sera faite dans l'esprit de ne retenir que les candidats ayant le meilleur profil en privilégiant l'expérience pertinente des candidats pour le poste qui sera notée à pas moins de 75 %.

A cette Phase, seuls les candidats ayant reçu une Note Minimale de 75% seront retenus.

Au cas où aucun des candidats n'aura totalisé la Note Minimale de 75%, il sera alors retenu les trois premiers parmi ceux ayant reçu une Note Supérieure ou Egale à 70%

(b) Phase d'interview des candidats présélectionnés sur 100 points.

L'interview sera notée sur 100 points

A la fin du processus, les candidats seront classés par ordre de mérite après pondération des différentes notes obtenues dans les 2 phases de la Sélection. La note du CV aura un poids de 70% et celle de l'interview 30% (le CV sera pondéré pour 70% et l'Interview pour 30%).