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 »

DEMANDE DE MANIFESTATION D'INTÉRÊT
(SERVICES DE CONSULTANTS)

SÉLECTION D'UN CONSULTANT INDIVIDUEL

N° du Projet : P176396/P180987

DON IDA N° E0930-BI/E2820-BI

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

Réf. STEP: BI-PAFEN-PIU-1222-CS-INDV

Le Gouvernement de la République du Burundi a reçu un Don de l'Association Internationale de Développement (IDA) pour financer le coût du Projet d'Appui aux Fondations de l'Economie Numérique (PAFEN) d'un montant de 92 millions de Dollars des Etats Unis.

L'objectif du 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 PAFEN est mis en œuvre à travers une Unité de Gestion du Projet (UGP) logée au sein du Secrétariat Exécutif des Technologies de l'Information et de la Communication (SETIC) qui est sous la tutelle du Ministère de la Communication, des Technologies de l'Information et des Médias.

Il est prévu qu'une partie des ressources de ce financement soit utilisée pour payer les prestations d'un **Consultant Informaticien Expert Sécurité Informatique** en faveur de « **Burundi Education and Research Network- BERNet** » dont les missions sont décrites dans les paragraphes suivants.

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

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

Les Termes de Références (TDRs) détaillés de la mission peuvent être obtenus à l'adresse indiquée ci-dessous.

Le projet PAFEN invite les consultants individuels admissibles à manifester leur intérêt à fournir les services décrits ci-dessus en fournissant les informations suivantes : une lettre de motivation et un curriculum vitae précisant la qualification du Consultant et l'expérience pertinente pour l'exécution des Services décrits ci-dessus, les expériences ou missions réalisées, les références similaires, en y annexant les copies légalisées des diplômes et attestations ainsi que tous autres documents justificatifs.

QUALIFICATIONS PROFESSIONNELLES ET ACADÉMIQUES

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);

L'attention des consultants intéressés est attirée sur la section III, paragraphes, 3.14, 3.16, 3.17 et 3.23 du « Règlement de Passation des Marchés pour les Emprunteurs sollicitant le Financement de Projets d'Investissement (FPI), Edition de Septembre 2023 relatifs aux règles de la Banque mondiale en matière de conflit d'intérêts et de l'éligibilité.

Un consultant individuel sera sélectionné en accord avec les procédures définies dans le Règlement de passation des marchés pour les Emprunteurs sollicitant le Financement des Projets d'Investissement (FPI), Edition de Septembre 2023.

Les Consultants intéressés peuvent obtenir des informations supplémentaires à l'adresse ci-dessous du Lundi au Jeudi de *8 heures 12 heures et de 14 heures à 17 heures 30 minutes et les Vendredi de 8h à 15 heures (heures locales)*.

Les manifestations d'intérêt doivent être livrées par écrit à l'adresse ci-dessous (en personne, ou par courrier, ou par e-mail) avant le **12 Avril 2024 au plus tard à 16 heures** *avec mention :*

« REPONSE A L'AVIS DE SOLLICITATION DE MANIFESTATIONS D'INTERET* N° BI-PAFEN-PIU-1222-CS-INDV » *POUR LE RECRUTEMENT D'UN CONSULTANT CHARGE DE LA SECURITE DU RESEAU INFORMATIQUE DE BURUNDI EDUCATION AND RESEARCH NETWORK – BERNET»

Attn: Monsieur le Coordonnateur du PAFEN

Boulevard Ndadaye Melchior, Building Orée du Golf, 4ème étage
E-mail: bienvenu.irakoze@pafen.gov.bi avec copie obligatoire à gaspard.mvukiye@pafen.gov.bi et pierre.ndamama@pafen.gov.bi et **belyse.ndayikeje@pafen.gov.bi**

Pour autorisation de publication

Bienvenu IRAKOZE

Coordonnateur du PAFEN