PRESIDENCE DE LA REPUBLIQUE

SECRETARIAT GENERAL

PRODIGY

PROjet de Gouvernance DIgitale et de Gestion de l'Identité MalagasY

Crédit 6780 - MG

APPEL A CANDIDATURES N° 044/23/PRODIGY/AMI

ASSISTANT(E) TECHNIQUE EXPERT EN CYBERSECURITE

1) Le Gouvernement de Madagascar a reçu un financement de l'Association Internationale de Développement (IDA) en vuede financer le PROjet de Gouvernance DIgitale et de Gestion de l'Identité MalagasY (PRODIGY), et a l'intention d'utiliser une partie du financement pour effectuer les paiements autorisés au titre du contrat d'un « **assistant(e) technique expert en cybersécurité**».
2) L'objectif général de la mission est de mettre en place une gouvernance de la sécurité pour permettre de définir une stratégie de sécurité efficace. Le consultant intervient en matière de prévention, de détection et de lutte contre la cybercriminalité. Ainsi, le consultant peut être appelé aux différents stades de "maturité digitale" des projets. En effet, il n'agit pas seulement à posteriori en réaction à un problème de sécurité informatique, ses rôles sont aussi et surtout, de donner à l'UGD toutes les clés de compréhension et d'anticipation face à une potentielle attaque informatique.
3) Le PRODIGY invite les candidats admissibles, à manifester leur intérêt. Ils doivent fournir les informations indiquant qu'ils possèdent les qualifications et expériences pour l'exécution de la prestation.
4) Un Consultant sera sélectionné en accord avec les procédures de la Banque mondiale définies dans le « Règlement de Passation des Marchés pour les Emprunteurs sollicitant le Financement de Projets d'Investissement (FPI), pour les Fournitures, Travaux, Services autres que des Services de Consultants et Services de Consultants » de Juillet 2016, réviséen Novembre 2017, Août 2018 et Novembre 2020.
5) Les Consultants intéressés peuvent obtenir des informations supplémentaires, y compris les Termes de Référence, à l'adresse ci-dessous. Les Termes de Référence peuvent être téléchargés sur ce lien **:** https://digital.gov.mg/tdr-ami-44/
6) Le Consultant doit disposer les qualifications et expériences suivantes :
   - Avoir cinq (05) ans d'expériences au moins et deux (02) expériences réussies dans la conduite de travaux similaires au cours des dix (10) dernières années ;
   - Avoir participé à au moins deux (02) projets dans le domaine d'analyse de risque et d'opportunités et de choix stratégiques ;
   - Capacités d'analyse et de rédaction avec une réelle expertise technique ;
   - Diplôme d'ingénieur ou équivalent (BAC + 5), avec une spécialisation en Sécurité des Systèmes d'Information et informatiques ou en réseaux et télécommunication
   - Ayant été formé en cybersécurité.
   - Maîtrise des normes et des procédures de sécurité, des outils et des technologies relatives à la sécurité informatique (ex: ISO/IEC 2700x notamment 27001, 27002, 27005 et 27032, COBIT 5, PCI-DSS etc.).
   - Solides connaissances des outils d'évaluation et d'analyse de risques (systèmes et réseaux) et des méthodologies (OWASP, EBIOS).
   - Ayant obtenu une certification de niveau international (OSCP, CISSP, CISM, …) serait un atout.
   - Ayant suivi une formation en DevSecOps et en pentest serait un atout.
   - Au moins 1 expérience dans le domaine de la sécurité des systèmes d'informations des services publics
   - Connaissances sur les normes et standards d'exploitation
   - Connaissance sur les législations en cybersécurité et cybercriminalité et en droit numérique
7) La durée du mandat du Consultant est prévue jusqu'à la fin du projet sous réserve d'une évaluation satisfaisante des performances du consultant après 3 mois puis de façon annuelle.
8) Les dossiers de candidature contenant (i) une lettre de motivation rédigée en français, (ii) un CV (modèle Banque mondiale) et (iii) les copies des diplômes, seront adressés à Monsieur le Coordonnateur du PRODIGY et envoyés au plus tard le **12 mai 2023** aux adresses suivantes :

   Courriel : **procurement@prodigy.gov.mg**

   copie à **coordonnateur@prodigy.gov.mg**

Et portant la mention « AMI N° 044/23 PRODIGY – Assistant(e) Technique Expert en Cybersécurité»

Antananarivo, le 13 avril 2023

Il est à noter que le projet PRODIGY s'engage activement dans la prévention de la Violence Basée sur le Genre notamment les divers abus, les harcèlements, l'exploitation sexuelle, la maltraitance et accorde une attention particulière à l'égalité des chances d'accès à l'emploi.

PRÉSIDENCE DE LA RÉPUBLIQUE

SECRETARIAT GENERAL

Projet de Gouvernance Digitale et de Gestion de l'Identité Malagasy
(PRODIGY)

Unité de Gouvernance Digitale (UGD)

Termes de référence

Assistant(e) Technique Expert en Cybersécurité

PTBA CODE : 2.1.5.6

1. CONTEXTE ET JUSTIFICATION :

Madagascar a reçu un financement de 143 millions de dollars américains, au travers du PROjet de Gouvernance DIgitale et de Gestion de l'Identité Malagasy (PRODIGY), qui est géré par une Unité de Coordination du Projet rattachée à la Présidence de la République de Madagascar. Ce financement doit permettre la modernisation ainsi que la transformation de l'administration publique à travers le pays.
Cette transformation passe par la rationalisation et la numérisation des services publics qui constituent les bases de la composante 2 du projet. Il s'agit d'augmenter l'offre, la couverture et la qualité des services publics, en renforçant les infrastructures et la capacité de l'administration à fournir des services publics plus rapides, moins chers et de meilleure qualité.
Ainsi les objectifs principaux sont de renforcer la capacité du gouvernement à rationaliser et à fournir des services publics par le biais de canaux multiples (par exemple, en ligne, par la voix, hors ligne), et de fournir une infrastructure institutionnelle et technologique (back-end et front-end) soutenant la fourniture de services.
La Présidence a créé une unité de gouvernance digitale (UGD) pour développer et coordonner la mise en œuvre de la stratégie nationale de gouvernance numérique. Cette stratégie est fondée sur les meilleures pratiques internationales, notamment une approche de conception agile et centrée sur l'utilisateur. L'UGD est dirigée par un Chief Digital Officer par interim (CDO) et composée d'une équipe pluridisciplinaire. Dans le cadre du renforcement de capacité du gouvernement à fournir des services selon des principes agiles et centrés sur l'utilisateur, l'Unité de Gouvernance Digitale a pour objectif d'accompagner chaque entité dans la transformation digitale de leurs processus.
Le manque de sécurisation des données et de respect de la vie privée ne favorise pas la confiance dans les services digitaux publics et privés et crée des risques pour tous les utilisateurs. Madagascar a adopté une loi sur la protection des données en 2014 (loi n° 2014-038) et une législation plus récente relative à la cybersécurité et la cybercriminalité a été adoptée en 2016 (loi n° 2016-031 amendant la loi n° 2014-006). Toutefois, les cadres réglementaires, opérationnels et institutionnels faisant toujours défaut, l'Équipe d'intervention en cas d'urgence informatique (« CIRT ») ainsi que l'autorité de protection des données connue sous le nom de Commission Malagasy de l'Informatique et des Libertés (« CMIL ») n'ont pu être établis. Le CIRT devrait être créé au sein de l'Autorité de Régulation des Télécommunications (ARTEC), tandis que la CMIL sera créée au sein du Ministère de la Justice, en étroite collaboration avec l'UGD. Aucune politique gouvernementale n'existe sur la propriété et l'utilisation des données, ni aucune autorité de surveillance opérationnelle garantissant la confidentialité des données. Les mesures techniques et organisationnelles de sécurisation des données à caractère personnel de la loi n° 2018-027 régissant les registres de l'état civil ne sont pas pleinement mises en œuvre. Le manque de formation des fonctionnaires accentue

également les risques de balayage massif de données. En conséquence, les systèmes digitaux publics de Madagascar figurent parmi les plus vulnérables au monde. Une Revue de la capacité en cybersécurité a été réalisée en 2016 par le Centre mondial des capacités de cybersécurité (GCSCC), relevant des lacunes et des défis importants.

Dans ce contexte, un assistant(e) technique (AT) Expert en Cybersécurité sera recruté afin de renforcer et d'appuyer l'UGD pour la mise en place des actions nécessaires à la correction ou à l'anticipation des menaces informatiques et pour garantir la sécurité des solutions développées, avec l'appui du PROjet de gouvernance DIgitale et de Gestion de l'identité MalagasY (PRODIGY).

2. DESCRIPTIF DU POSTE

a. Objectif(s)s de la mission

L'assistant(e) Technique sera chargé(e) de mettre en place une gouvernance de la sécurité pour permettre de définir une stratégie de sécurité efficace.
Le consultant(e) intervient en matière de prévention, de détection et de lutte contre la cybercriminalité. Ainsi, le consultant(e) peut être appelé(e) aux différents stades de "maturité digitale" des projets. En effet, il n'agit pas seulement à posteriori en réaction à un problème de sécurité informatique, ses rôles sont aussi et surtout, de donner à l'UGD toutes les clés de compréhension et d'anticipation face à une potentielle attaque informatique.

b. Tâches et étendue de la mission

Sous la supervision du Chief Digital Officer, l'Assistant(e) Technique a pour mission principale de :

- Faire un audit permanent du niveau de sécurité des systèmes informatiques, des applications ou de tout autre point d'entrée pouvant provoquer une attaque ;
- Élaborer des plans d'actions très précis en cas d'attaque ;
- Définir les règles de sécurité applicatives en réponse aux exigences fixées par des référentiels de bonnes pratiques ou par des réglementations propres à l'activité de l'UGD.

Sur le plan opérationnel, l'Assistant(e) technique sera en charge de :

- Superviser en toute confidentialité les solutions hébergées sur l'environnement de l'UGD ;
- Détecter, analyser et qualifier les incidents, les menaces et les cyberattaques ;
- Garantir l'analyse des différentes données informatiques ;
- Orienter les équipes techniques pour sécuriser le réseau et les systèmes informatiques ;
- Rédiger des procédures de sécurité adaptées et sensibiliser aux enjeux de la sécurité du réseau, de la data et des systèmes informatiques.

Sur le plan stratégique et organisationnel :

- Assurer une veille continue sur les menaces actuelles ;
- Documenter les bases de connaissances et procédures de traitement ;
- Suivre constamment la vulnérabilité software et hardware ;
- Analyser les malwares et l'ensemble des violations de données.

c. Livrables et Résultats attendus

- Cartographie des risques de sécurité ;
- Document d'audit de sécurité ;
- Document des recommandations et des mesures préventives et correctives avec les plans d'actions ;

- Documents relatifs aux :
    - Politique sécurité des systèmes d'information ;
    - Guide de sécurité des systèmes d'informations.

3. CRITÈRES DE QUALIFICATION DU CONSULTANT

a. EXPERIENCES

- Avoir 5 ans d'expériences au moins et deux (02) expériences réussies dans la conduite de travaux similaires au cours des dix (10) dernières années ;
- Avoir participé à au moins 2 projets dans le domaine d'analyse de risque et d'opportunités et de choix stratégiques ;
- Capacités d'analyse et de rédaction avec une réelle expertise technique ;

b. COMPETENCES

- Diplôme d'ingénieur ou équivalent (BAC + 5), avec une spécialisation en Sécurité des Systèmes d'Information et informatiques ou en réseaux et télécommunication
- Ayant été formé en cybersécurité.
- Maîtrise des normes et des procédures de sécurité, des outils et des technologies relatives à la sécurité informatique (ex: ISO/IEC 2700x notamment 27001, 27002, 27005 et 27032, COBIT 5, PCI-DSS etc.).
- Solides connaissances des outils d'évaluation et d'analyse de risques (systèmes et réseaux) et des méthodologies (OWASP, EBIOS).
- Ayant obtenu une certification de niveau international (OSCP, CISSP, CISM, …) serait un atout.
- Ayant suivi une formation en DevSecOps et en pentest serait un atout.

c. COMPETENCES TRANSVERSES SOUHAITEES :

- Au moins 1 expérience dans le domaine de la sécurité des systèmes d'informations des services publics
- Connaissances sur les normes et standards d'exploitation
- Connaissance sur les législations en cybersécurité et cybercriminalité et en droit numérique

4. RAPPORTS A FOURNIR ET CALENDRIER

Il est attendu de l'Assistant(e) Technique de fournir un reporting régulier et périodique sur l'état d'avancement du projet, ainsi que tout document qui peut rapporter l'état d'avancement des projets aux personnes concernées de l'UGD.

Le consultant sera tenu de fournir un rapport d'activité mensuel en version physique et électronique des activités réalisées conformément à leurs termes de référence, pour envoi au coordonnateur de projet.

5. DURÉE DE LA MISSION

Les mandats du consultant sont prévus se tenir jusqu'en Décembre 2024 avec une évaluation annuelle positive de sa prestation. Le consultant sera basé à Antananarivo.

Annexe

Modèle de Curriculum vitae

CURRICULUM VITAE (CV)

Titre du Poste :	*[Insérer le titre du poste]*
Nom de l'expert :	*Mr ou Mme ou Mlle [Insérer le nom complet]*
Adresse physique	
Date de naissance :	*[Jour/mois/année]*
Nationalité/Pays de résidence	

Etudes : *[Résumer les études universitaires et autres études spécialisées suivies, en indiquant le nom de l'école ou université, les années d'étude et les diplômes obtenus]*

Expérience professionnelle pertinente à la mission : *[Dresser la liste des emplois exercés depuis la fin des études, dans un ordre chronologique inverse, en commençant par le poste actuel ; pour chacun, indiquer les dates, le nom de l'employeur, le titre professionnel de l'employé et le lieu de travail ; pour les emplois des dix dernières années, préciser en outre le type de travail effectué et fournir, le cas échéant, les noms des clients à titre de références. Les emplois tenus qui sont sans rapport avec la mission peuvent être omis.]*

Période	**Nom de l'employeur, titre professionnel/poste tenu. Renseignements sur contact pour références**	**Pays**	**Sommaire des activités réalisées, en rapport avec la présente mission**
[par ex. Mai 2011-présent]	*[par ex. Ministère de ……, conseiller/consultant pour…* *Pour obtenir références :* *Tél……../courriel…… ;* *M. xxxx, Directeur]*		

Langues pratiquées (indiquer uniquement les langues dans lesquelles vous pouvez travailler) : ____

Compétences/qualifications pour la mission :

Tâches spécifiques incombant au consultant parmi les tâches à réaliser :	**Référence à des travaux ou missions antérieures illustrant la capacité de l'expert à réaliser les tâches qui lui seront attribuées**

Renseignements pour contacter le consultant :
(courriel _____ , téléphone _____)

Certification :
Je soussigné, certifie que le présent CV me décrit de manière correcte, ainsi que mes qualifications et mon expérience professionnelle ; je m'engage à être disponible pour réaliser la mission lorsque cela sera nécessaire, au cas où le contrat serait attribué. Toute fausse déclaration ou renseignement fourni incorrectement dans le présent CV pourra justifier ma disqualification ou mon renvoi par le Client, et/ou des sanctions par la Banque.

[jour/mois/année]

_____

Nom du consultant Signature Date