APPEL A CANDIDATURE D'UN RESPONSABLE DE CYBER SECURITE DU SYSTEME D'INFORMATION

Guinéenne de Monétique (GuiM) est un Groupement qui regroupe la Banque Centrale et l'ensemble des établissements de crédit, et dont le siège se trouve à Conakry en République de Guinée.

Elle a pour objet, la mise en place du Switch monétique et digital.

Dans ce cadre, la GuiM recrute :

- **Responsable de Cyber Sécurité du Système d'Information**.

Conditions Générales :

Pour être éligible, les candidats doivent remplir les conditions suivantes :

- Être disponible immédiatement ;
- Être âgés de 30 ans au plus ;
- Avoir la nationalité Guinéenne.

Le candidat retenu sera engagé sous un Contrat à Durée Indéterminé (CDI), assorti d'une période d'essai de trois (3) mois.

Les dossiers de candidatures (lettre de motivation CV, diplôme et/ou attestations, attestations de travail, prétentions salariales, etc.…) devront parvenir par voie électronique à : **adama.mbaye@apb-guinee.org au plus tard le vendredi 12 avril 2024 à 12h (GMT).**

TERMES DE REFERENCE DU POSTE

Référence	**RCSSI**
Poste proposé	Responsable de Cyber Sécurité du Système d'Information
Contrat	CDI avec période d'essai de trois (3) mois.
Employeur	Guinéenne de Monétique (GuiM)
Salaire	Négociable en fonction de l'expérience
Localisation	Poste basé à Conakry en République de Guinée

MISSION PERMANENTE DU POSTE

La Guinéenne de Monétique (GuiM) est un GIE qui a pour mission principale la mise en place et la gestion du switch monétique et digital de la République de Guinée, qui, par le présent appel d'offre international, recherche un Responsable de Cyber Sécurité du Système d'Information.

CONDITIONS GENERALES :

Missions	- **Responsable de la définition de la politique de sécurité du système d'information le cas échéant (prévention, protection, défense, résilience/remédiation) et de son application. Il assure son rôle de conseil, d'assistance, d'information, de formation et d'alerte, en particulier auprès des directeurs métiers, DG ;** - **Il préconise, voire prend, toute décision d'intervention sur les systèmes d'information et télécoms de son périmètre, en cas d'attaques potentielles ou avérées.**

Description des activités principales	- Analyser et évaluer les risques associés à la sécurité du SI ; - Définir et faire évoluer la politique de sécurité des systèmes d'information de l'entreprise (PSSI) ; - Etablir un plan de prévention des risques informatiques et un plan de continuité d'activité (PCA) ; - Participer à la définition et au contrôle de la gestion des habilitations ; - Mettre en place les méthodes et outils de sécurité adaptés, et accompagner leur implémentation auprès des utilisateurs ; - Assurer une veille technologique et règlementaire pour garantir la sécurité logique et physique du SI dans son ensemble ; - Animer et gérer son équipe ; - Responsabiliser ses équipes en leur définissant des objectifs clairs, en les challengeant et en validant les plans d'actions proposés par ces derniers ; - Développer les compétences des collaborateurs sous sa responsabilité ; - Veiller à la rédaction et mise à jour des procédures ; - Veiller au respect des procédures, normes et standards de travail de la GuiM ; - Veiller à la mise à jour des fiches de postes de son périmètre.
Relations intérieures et extérieures	- Ensemble du personnel ; - Membre de la GuiM, Clients, consultants, prestataires, partenaires (nationaux et étrangers), commissaires aux comptes, organisations sociales, assurances, structures de santé.
Qualifications requises	**Formation académique** Avoir un Bac+5 Ingénieur, informatique. **Expériences professionnelles pertinentes** - Avoir 10 ans d''expériences IT dans le domaine de la sécurité ; - Avoir des certifications de types CISA, CISM, CISSP ; - Bonne connaissance des principaux prestataires de la cybersécurité ; - Bonne connaissance des normes et procédures classique en termes de sécurité (antivirus, firewall, cryptographie, etc.) ; - Bonne connaissance de réseau et système ; - Bonne connaissance des outils d'évaluation et maîtrise des risques (EBIOS, MEHARI, etc.) ; - Bonne connaissance des normes et standards de sécurité (ISO27001, PCI-DSS, NIST CSF, CIS20, etc.) ; - Bonne connaissance des méthodologies d'audit (e g. OWASP, OSSTMM, etc.) ; - Connaissance juridique de base et de droit informatique. **Compétences et qualités requises** - Capacité de motivation et de management d'équipe ; - Pilotage par objectifs ; - Gestion du stress ; - Réactivité, relationnel, communication ;

	- Ethique, sens et respect de la confidentialité ; - Planification et organisation du travail ; - Aisance relationnelle ; - Ecoute, compréhension des autres, Esprit de médiateur ; - Esprit d'initiative - Maîtrise de l'Anglais.

NB : **Pour les envois par mail, toutes les pièces demandées, doivent être scannées puis transformées en PDF. Les originaux vous seront réclamés lors de l'entretien.**

La Direction Générale