KKM/KTN
MINISTERE D'ETAT,
MINISTERE DE LA FONCTION PUBLIQUE
ET DE LA MODERNISATION DE L'ADMINISTRATION

CABINET

LE DIRECTEUR DE CABINET

REPUBLIQUE DE COTE D'IVOIRE
Union-Discipline-Travail

Abidjan, le 29 OCT 2024

002250/MEMFPMA/DGFP/DFRC

COMMUNIQUE

L'Organisation pour l'Interdiction des Armes Chimiques (OIAC) lance un avis de vacance pour le poste de **Spécialiste de la sécurité de l'information** (P-3), Division : Bureau de la confidentialité et de la sécurité.

Les critères de sélection et les conditions à remplir sont joints au présent communiqué.

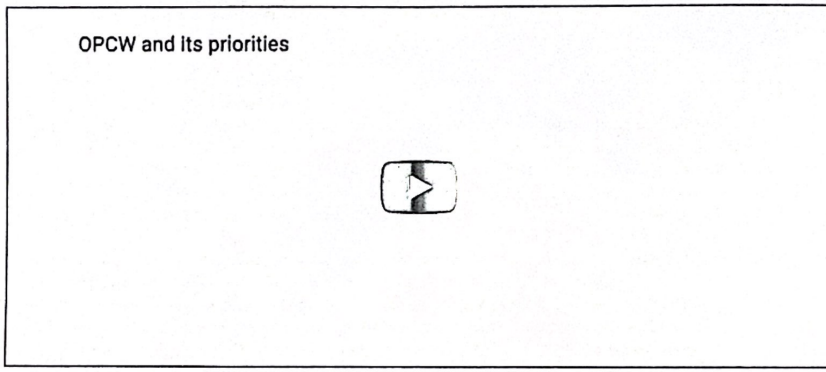
Les fonctionnaires désireux de faire acte de candidature, sont invités à consulter les détails du poste ainsi que la procédure de soumission des candidatures, au plus tard **le 13 novembre 2024**, via le lien ci-dessous : **https://jobs.ocpw.org/job/print-job-form-information-security-officer-p-3-_448.aspx**

Pièce Jointe :
-avis de vacance de poste.

Nasséré KABA

Spécialiste de la sécurité de l'information (P-3)

Qui sommes-nous



Le Bureau de la confidentialité et de la sécurité relève du Cabinet du Directeur général.
La Section de la sécurité des opérations est chargée de fournir des lieux de travail sûrs et de protéger les biens de l'OIAC.

La Section de la confidentialité et de la sécurité de l'information est chargée de la protection des systèmes d'information et de communication et assiste les États parties et le Secrétariat dans la mise en œuvre du régime de confidentialité.

Informations générales

- **Type de**
  contrat Professionnel à durée déterminée
- **Classe**
  P3
- **Rémunération mensuelle estimée en fonction de l'indemnité de poste et de la situation familiale :** 8 298 USD
- **Date**
  de clôture 13/11/2024

Responsabilités
Résumé du poste
Le Bureau de la confidentialité établit le cadre, fournit les lignes directrices, institue les mesures et met en œuvre les dispositions nécessaires pour garantir et faire respecter le régime strict de confidentialité de l'OIAC ; la sécurité opérationnelle des biens du Secrétariat ; la sécurité de tous ses systèmes électroniques ; la confidentialité de tous les documents classifiés et leur sauvegarde. Alors que le régime de sécurité pour la protection du personnel, des biens, des opérations et de l'information relève de la responsabilité et des principaux objectifs de l'OCS, plus largement, l'OCS assure la gestion de la sécurité à l'appui de toutes les missions, enquêtes et activités de l'OIAC.

La Section de la confidentialité et de la sécurité de l'information est chargée de mettre en œuvre et de gérer le régime de confidentialité et le programme de sécurité de l'information, en conseillant et en supervisant tous les aspects de la sécurité de l'information de tous les processus opérationnels et des fonctions et responsabilités liées à l'information, à la communication et à la technologie (TIC).

Principales responsabilités

Sous la supervision générale du Chef de la Section de la confidentialité et de la sécurité de l'information, le (la) titulaire s'acquitte des fonctions suivantes :

Coordonner tous les aspects du programme de sécurité de l'information de l'OIAC avec la gestion et la mise en œuvre quotidiennes de l'information et des mesures de sécurité des TIC afin d'assurer la préservation de la confidentialité, de l'intégrité et de la disponibilité des informations de l'OIAC.

- Servir de point focal pour la sécurité de l'information au niveau technique détaillé pour tous les programmes et projets liés à la sécurité de l'information et conseiller le Chef de la confidentialité et de la sécurité de l'information sur toutes les questions liées à la sécurité de l'information ;
- Veiller à ce que la conformité aux normes organisationnelles et sectorielles pertinentes (c'est-à-dire ISO 27001) soit maintenue pour tous les systèmes et actifs ICT ;
- Élaborer et tenir à jour des politiques, des procédures, des normes et des lignes directrices relatives à la sécurité de l'information pour des TIC sécurisées afin de soutenir le mandat de l'OIAC en maintenant un équilibre adéquat entre des contrôles efficaces de la confidentialité et de la sécurité de l'information et un accomplissement efficace et sans entrave des tâches de l'OIAC ;
- Communiquer et appliquer les politiques, procédures, normes et directives de sécurité de l'information à tout le personnel et aux parties prenantes concernées ;
- Effectuer et examiner des audits de sécurité des fournisseurs de services TIC, afin d'inclure l'ensemble de la chaîne d'approvisionnement, conformément aux accords contractuels pertinents ;
- Effectuer une surveillance de sécurité régulière de tous les réseaux (connectés à Internet et non connectés à Internet), y compris l'identification des fonctions critiques et des vulnérabilités conformément aux politiques et procédures pertinentes ;
- Collaborer avec les membres du personnel des autres branches/unités et les parties prenantes concernées pour fournir des conseils sur les exigences en matière de confidentialité et de sécurité de l'information afin de s'assurer que l'Organisation est conforme aux normes de sécurité ;
- Surveiller l'accès des utilisateurs sur tous les réseaux en veillant à ce que l'accès aux informations confidentielles et sensibles soit conforme à celui autorisé dans le cadre des politiques et procédures pertinentes.
- Veiller à ce que les actifs TIC soient gérés et surveillés pour assurer la mise en place de mesures de sécurité efficaces ;
- Participer aux activités liées aux changements apportés à l'organisation, aux processus opérationnels, aux installations et aux systèmes de traitement de l'information pour s'assurer que les contrôles internes sont en place.

Pour consulter la description complète du poste, veuillez cliquer ici.

Qualifications et expérience

Éducation

Essentiel:

- Diplôme universitaire supérieur en sécurité de l'information ou dans une discipline apparentée ;
- Un diplôme universitaire de premier cycle dans toutes les matières pertinentes combiné à une expérience pertinente (minimum 7 ans) peut être accepté à la place du diplôme universitaire spécifié.

Certification requise :

- Certifications sectorielles pertinentes (par exemple, CISSP, CISM, CCSP, etc.)

Certification souhaitable :

- CRISC, GIAC, certifications des fournisseurs, administration du réseau, etc.

Connaissances et expérience

Essentiel:

Au moins 5 ans d'expérience professionnelle pertinente dans la profession de la sécurité de l'information (minimum 7 ans avec un diplôme universitaire de premier cycle) avec une expérience significative dans la mise en œuvre de la sécurité de l'information, y compris une expérience pratique dans les domaines suivants :

- Concevoir des solutions de sécurité TIC ;
- Expérience de la surveillance des incidents et des enquêtes de sécurité ;
- Expérience de l'assistance et de la réalisation d'évaluations des risques de sécurité ;
- Expérience dans le conseil et les tests de sécurité des environnements TIC ;
- Administration et surveillance du pare-feu ;
- Expérience dans la supervision d'opérations au sein d'environnements sécurisés et de systèmes de traitement de l'information ;

Souhaitable:

- Expérience de la gestion des autorités de certification, de la sécurité de Microsoft Office 365, de la sécurité du cloud et de l'investigation numérique ;
- Expérience dans une organisation internationale.

Aptitudes et compétences

Aptitudes (compétences clés) :

- Connaissance des principes et des meilleures pratiques en matière de sécurité de l'information ;
- Connaissance des normes et des cadres de l'industrie (par exemple, NIST, ISO 27001, etc.)
- Expérience dans l'élaboration et la rédaction de politiques liées à la sécurité de l'information.
- Expérience pratique de l'utilisation d'outils et de technologies de sécurité de l'information (p. ex., SIEM, IDS/IPS, antivirus, pare-feu, etc.) ;
- Excellentes compétences analytiques et de conceptualisation et capacité à planifier et à organiser des processus complexes ;
- Excellentes compétences interpersonnelles, d'entrevue et de négociation ;
- Excellentes compétences en communication, avec une capacité démontrée à présenter des informations clairement et logiquement, tant verbalement qu'à l'écrit ;
- Aptitude avérée à rédiger, réviser et présenter des documents en anglais ;
- Capacité d'agir avec discrétion et tact dans des situations délicates ;
- Capacité à bien travailler en équipe avec des personnes d'origines nationales/culturelles différentes.

Other Skills:

- Diplomacy and demonstrated ability to work in an international organisation with diverse cultures.

Languages

Fluency in English is essential and a good working knowledge of one of the other official languages (Arabic, Chinese, French, Russian, and Spanish) is desirable.

Additional Information

This fixed-term appointment is for the duration of two years with a six-month probationary period, and is subject to the OPCW Staff Regulations and Interim Staff Rules.

The OPCW is a non-career organisation with limited staff tenure. The total length of service for Professional staff shall not exceed 7 years.

The mandatory age of separation at the OPCW is 65 years.

This fixed-term appointment is for the duration of two years with a six-month probationary period, and is subject to the OPCW Staff Regulations and Interim Staff Rules.

The OPCW is a non-career organisation with limited staff tenure. The total length of service for Professional staff shall not exceed 7 years.

The mandatory age of separation at the OPCW is 65 years.

The Director-General retains the discretion to not make any appointment to this vacancy, to make an appointment at a lower grade, or to make an appointment with a modified job description. Several vacancies may be filled.

Only fully completed applications submitted before the closing date and through OPCW CandidateSpace will be considered. Only applicants under serious consideration for a post will be contacted.

Fixed-term staff members participate in the OPCW Provident Fund. A monthly staff contribution is met with a doubled amount by the OPCW under the provisions for social security. As the OPCW is exploring membership of the United Nations Joint Staff Pension Fund (UNJSPF), staff participation in the Provident Fund may be replaced by participation in the UNJSPF effective 1 January 2025.

Applications from qualified female candidates are strongly encouraged.

OPCW General Terms and Conditions

Important notice for applicants who are currently insured under the Dutch Social Security system

Although headquartered in the Netherlands, the OPCW is not a regular Dutch employer but a public international organisation with its own special status. Please be advised that if you are currently insured under the Dutch Social Security system, you will be excluded from this system as a staff member of the OPCW. You will consequently be insured under the organisation's system. The above also applies to your dependents unless they are employed by a regular Dutch employer, they are self-employed in the Netherlands, or are receiving Dutch social security payments.

Please refer to the website of the Ministry of Social Affairs and Employment for more information about the possible consequences for you and your dependents, such as exclusion from 'AWBZ' and 'Zorgverzekeringswet' coverage: 'Werken bij een internationale organisatie'.