



Secrétariat général (SG)

Genève, le 12 décembre 2025

Courriel: HRerecruit@itu.int

A l'attention de la Direction générale

Lettre circulaire N° 25/60

Sujet: **AVIS DE VACANCE No. 2231P-2025/BDT-DNE/EXTERNE/P3 "Responsable des données et des politiques en matière de cybersécurité"**

Madame, Monsieur,

L'emploi décrit en annexe doit être pourvu au siège de l'UIT.

La description d'emploi correspondante, les aptitudes requises des candidats, ainsi que toutes indications utiles, figurent en annexe à la présente lettre.

Les Administrations sont priées de diffuser les avis de vacance à toutes les sources potentielles de recrutement : universités, instituts, associations d'ingénieurs et le secteur privé selon le cas.

Je serais reconnaissant à votre Administration de bien vouloir inciter les candidats et notamment les candidates qualifié(e)s à soumettre leur candidature pour l'emploi mentionné ci-dessus, au plus tard le 12/02/2026 sur notre site carrière :

Responsable des données et des politiques en matière de cybersécurité

La Conférence de plénipotentiaires a adopté la Résolution 48 (Rev. Dubaï 2018), décidant que : « ... lorsque des emplois vacants sont pourvus par recrutement international, lors du choix entre plusieurs candidats ayant les qualifications requises pour l'emploi, la préférence doit être donnée aux candidats des régions du monde qui sont sous-représentées dans les effectifs de l'Union, compte tenu de l'équilibre entre le personnel féminin et le personnel masculin prescrit dans le régime commun des Nations Unies ; ».

Veuillez agréer, Madame, Monsieur, l'assurance de ma haute considération.

Doreen Bogdan-Martin
Secrétaire générale

Annexes : **2231P-2025/BDT-DNE/EXTERNE/P3 "Responsable des données et des politiques en matière de cybersécurité"**

Job Title: Responsable des données et des politiques en matière de cybersécurité

UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

L'UIT - principale institution des Nations Unies pour les technologies de l'information et de la communication - a pour tâche de connecter le monde. A cette fin, elle gère sur le plan international le spectre des fréquences radioélectriques et les orbites de satellites, s'emploie à renforcer l'infrastructure des communications dans les pays en développement et élabore des normes mondiales qui garantissent la parfaite interconnexion de systèmes de communication très divers. L'UIT organise également les manifestations mondiales TELECOM, qui rassemblent les représentants les plus éminents des secteurs public et privé et favorisent les échanges d'idées et de connaissances, dans l'intérêt de tous.

L'UIT applique une politique de tolérance zéro à l'égard de toute forme de harcèlement. L'UIT s'est engagée en faveur de la diversité et de l'intégration au sein de son effectif, et encourage tous les candidats quels que soient leur sexe, leur nationalité, leurs origines religieuses et ethniques, y compris les personnes handicapées, à postuler pour faire partie de l'organisation. La parité des genres est d'une grande importance pour l'UIT.

Responsable des données et des politiques en matière de cybersécurité

Numéro de l'avis de vacance: 2231

Secteur: BDT

Département: DNE

Pays du contrat: Suisse

Lieu d'affectation: Genève

Numéro de poste: TD32P30750

Grade: P3

Type de contrat: Durée déterminée

Durée du contrat: 2 ans avec possibilité de prolongation

Type de publication: Externe

Date limite de candidature (Minuit heure de Genève) 12 Février 2026

UNITE ORGANISATIONNELLE

Le Bureau de développement des télécommunications (BDT) est responsable de l'organisation et de la coordination des travaux du Secteur du développement des télécommunications de l'Union (UIT-D). Le BDT s'occupe principalement des politiques, des stratégies, des programmes et des projets de développement, ainsi que des activités de coopération technique visant à favoriser et à encourager l'accès universel, à un coût abordable, à des télécommunications/technologies de l'information et de la communication (TIC) sûres et de qualité, et à encourager une utilisation équitable et inclusive des télécommunications/TIC pour mobiliser les personnes et les sociétés en faveur du développement durable. Afin de répondre de manière efficace et rationnelle aux besoins des États Membres, le BDT est divisé en quatre départements fonctionnels:

- Département de la coordination des opérations (Bureau de l'Adjoint au Directeur)
- Département des projets, des partenariats et des compétences numériques (PPS)
- Département des réseaux numériques et de l'environnement (DNE)
- Département de la société de connaissances numériques (DKS)

Le département des réseaux numériques et de l'environnement (DNE) est chargé d'aider les États Membres, en particulier les pays du G77, à relever un large éventail de défis en matière de développement des TIC, tels que la connectivité de base, la gestion du spectre, l'évolution des réseaux et des technologies à large bande actuels et futurs, la mise en œuvre d'un accès universel

et financièrement abordable et le renforcement de la sécurité grâce à l'appui à la cybersécurité. En outre, le département DNE fournit les compétences spécialisées et l'appui nécessaire pour les télécommunications d'urgence et les aspects de plus en plus importants et urgents liés à l'environnement et aux changements climatiques.

CONTEXTE ORGANISATIONNEL

Le poste est à pourvoir au sein de la Division de la cybersécurité du Bureau de développement des télécommunications (BDT), qui joue un rôle de premier plan dans les activités menées par l'UIT pour renforcer les capacités et la résilience en matière de cybersécurité, en particulier dans les pays en développement. La Division gère des initiatives d'envergure mondiale, telles que l'Indice mondial de cybersécurité (GCI), l'élaboration de stratégies nationales en matière de cybersécurité, la protection en ligne des enfants et les programmes régionaux de renforcement des capacités. Elle joue également un rôle crucial dans le renforcement de la coopération internationale, l'intégration des politiques de cybersécurité et la prise de décisions fondées sur des données probantes dans le cadre du programme de développement du numérique.

Le/la responsable fournit un appui à la Division dans l'exécution de son mandat, en assumant un portefeuille équilibré de responsabilités comprenant l'évaluation de la cybersécurité, l'analyse des données, l'engagement des parties prenantes et la coordination stratégique. L'un des principaux rôles du/de la titulaire est de gérer la mise en œuvre de l'Indice mondial de cybersécurité (GCI), qui est l'outil d'évaluation comparative de référence de l'UIT visant à mesurer les engagements des États Membres en matière de cybersécurité et à favoriser le dialogue international. Parallèlement, le/la titulaire contribue à la conception et à la mise en œuvre de projets au niveau des divisions, d'initiatives régionales et d'initiatives menées à l'échelle de l'UIT concernant les politiques en matière de cybersécurité, le renforcement des capacités, les statistiques et les retombées des technologies émergentes. Le/la titulaire travaillera en collaboration étroite avec les bureaux régionaux de l'UIT, les consultants, les États Membres et les partenaires extérieurs pour garantir la qualité, la cohérence et la visibilité des travaux de l'UIT dans le domaine de la cybersécurité. Le/la responsable des données et des politiques en matière de cybersécurité contribue également à la coordination interne entre le BDT et l'UIT au sens large, afin de promouvoir des approches intégrées et innovantes en matière de cybersécurité, dans le cadre des priorités de l'Union en matière de développement du numérique. Le/la titulaire travaille sous la supervision du Chef de la Division de la cybersécurité et peut fournir des orientations au personnel moins expérimenté et aux consultants.

TÂCHES ET RESPONSABILITÉS

Le/la titulaire:

- Organise, planifie et coordonne la mise en œuvre de l'Indice mondial de cybersécurité (GCI), y compris ses mises à jour périodiques, la collecte de données, la validation, l'analyse, l'élaboration de rapports et l'établissement de rapports ad hoc; supervise et coordonne le travail des consultants qui participent à la collecte et à la validation des données.
- Organise et planifie le travail correspondant des Bureaux régionaux de l'UIT, et communique avec eux, fournit un appui aux coordonnateurs régionaux en matière de cybersécurité et aux États Membres dans la planification, la mise en œuvre et le suivi des activités et des projets liés à l'indice GCI, y compris en coordonnant la fourniture d'une formation technique et d'autres produits et initiatives connexes.
- Contribue à la conception, à la planification et à l'exécution des activités relevant des projets et des initiatives de la Division, selon les besoins. Mène des études et examine l'évolution des technologies en matière de cybersécurité; étudie les évolutions et les tendances relatives aux bonnes pratiques, aux politiques et aux aspects de conformité en matière de cybersécurité, conformément aux domaines prioritaires définis par l'UIT-D et à la stratégie globale de l'UIT en matière de cybersécurité.
- Fournit des contributions et formule des avis sur les statistiques et indicateurs de cybersécurité de l'UIT afin d'améliorer la qualité et la pertinence des données. Procède à l'analyse requise des projets liés à la cybersécurité et faisant intervenir des études de faisabilité et l'analyse des systèmes, afin de faciliter la conception, le développement et la mise en œuvre des services et des fonctionnalités devant être fournis aux États Membres.
- Assure la liaison avec les partenaires extérieurs, les orateurs et les modérateurs des sessions pour coordonner l'élaboration du contenu, les supports, les délais, la logistique des manifestations et la mise à jour des sites web pertinents; organise des réunions et établit des rapports sur les résultats.

- Rédige des propositions, des présentations, des notes d'allocution, des notes d'information et des documents d'information pour appuyer la coordination interne et l'engagement stratégique externe.
- Facilite la participation de l'UIT aux mécanismes de coordination des Nations Unies et aux initiatives ad hoc relatives aux technologies émergentes et à la cybersécurité. Fournit un appui afin d'identifier des partenaires potentiels parmi les parties prenantes concernées, y compris parmi les gouvernements, les organisations internationales et le secteur privé.
- Effectue des recherches et suit les initiatives en faveur de la participation des États Membres, en recensant les possibilités de collaboration à l'échelle des projets et des programmes. Élabore les ordres du jour des manifestations, organise les réunions et fournit des rapports sur les réunions/manifestations. Si nécessaire, participe à des réunions et séminaires nationaux, régionaux et internationaux sur la cybersécurité et présente des exposés.
- Participe à la rédaction de documents écrits, notamment de documents de travail, de notes analytiques, de rapports et de présentations à usage interne et externe. Conçoit, planifie et gère la mise en œuvre des projets et assure une coordination avec le personnel de l'UIT, les techniciens des États Membres, les fournisseurs de solutions et les partenaires afin d'assurer une mise en œuvre efficace. Contribue à l'achat d'équipements et de services pour appuyer l'exécution des projets.
- Contribue à la collaboration transversale entre le BDT et l'UIT au sens large pour faciliter la planification et la mise en œuvre intégrées des activités liées à la cybersécurité. Fournit un appui pour la planification et l'exécution des activités de cybersécurité dans les délais impartis et avec précision, tout en garantissant la fourniture de résultats de qualité. Contribue aux activités de planification budgétaire et de gestion des dépenses du programme afin d'obtenir des résultats significatifs.
- Effectue des missions.
- S'acquitte de toute autre tâche connexe qui peut lui être confiée.

COMPETENCES ESSENTIELLES

Application des connaissances spécialisées; Aptitude à communiquer efficacement; Formation et échange de connaissances; Engagement à l'égard de l'organisation; Approche axée sur les résultats; et, Esprit d'équipe et collaboration.

COMPETENCES FONCTIONNELLES

Analyse, sûreté de jugement et aptitude à décider

Souci du client et de la prestation de services

Qualités de chef

Etablissement de réseaux et de partenariats

Aptitude à planifier et à organiser

COMPETENCES TECHNIQUES

- Bonne connaissance des questions de cybersécurité et de politique du numérique, y compris des cadres de coopération internationale et du rôle des outils de référence tels que l'Indice mondial de cybersécurité (GCI).
- Solides compétences en gestion de projet, notamment en matière de planification, d'exécution, de suivi et d'établissement de rapports, et aptitude à gérer plusieurs priorités en travaillant sous pression et à respecter des délais serrés.
- Excellente aptitude à communiquer et à mobiliser les parties prenantes, et aptitude à assurer une coordination efficace avec les États Membres, les bureaux régionaux, les partenaires et les équipes internes.
- Compétences avérées en matière de rédaction et d'édition, et capacité à établir des rapports, des présentations et des documents d'information clairs, concis et cohérents sur le plan technique.
- Aptitude avérée à résoudre des problèmes et à s'adapter dans des contextes dynamiques, en adoptant une approche axée sur les résultats, et capacité à travailler à la fois de façon indépendante et en équipe.
- Haut niveau de professionnalisme et d'intégrité, sens aigu des responsabilités, volonté d'obtenir des résultats de qualité et motivation en adéquation avec les objectifs de l'Organisation.

QUALIFICATIONS REQUISÉS

Education:

Diplôme universitaire supérieur en mathématiques, en relations internationales, en gestion de l'information ou dans un domaine connexe ou dans un domaine connexe OU formation reçue dans un établissement d'enseignement supérieur de réputation établie, sanctionnée par un diplôme de niveau équivalent à un diplôme universitaire supérieur dans l'un des domaines précités.

Pour les candidats internes, un titre universitaire de premier cycle dans l'un des domaines précités, associé à sept années d'expérience professionnelle pertinente, peut remplacer le titre universitaire supérieur à des fins de promotion ou de rotation.

Expérience:

Au moins cinq années d'expérience à des postes à responsabilité croissante dans le domaine de la cybersécurité, en particulier concernant les politiques en matière de cybersécurité, l'élaboration de stratégies et la transformation numérique, dont au moins deux ans au niveau international.

Expérience de la gestion ou de la contribution à des initiatives axées sur les données ou à des indices mondiaux évaluant l'état de préparation des pays ou des secteurs à la cybersécurité.

Une expérience avérée de la gestion de projets, y compris de la planification, de la coordination et de la mise en œuvre d'initiatives en collaboration avec diverses parties prenantes, est essentielle.

Une expérience de la collaboration avec les pays en développement, y compris les pays les moins avancés (PMA) et les petits États insulaires en développement (PEID), dans le contexte de l'appui aux politiques, du renforcement des capacités ou de la mobilisation multi-parties prenantes, est également nécessaire. Expérience avérée de la collecte, de la validation et de l'analyse de données, avec une capacité à garantir l'exactitude des données, à interpréter les résultats et à appuyer la prise de décisions fondées sur des données probantes.

Un doctorat dans un domaine connexe peut être considéré comme équivalent à deux années d'expérience professionnelle.

Langues:

Connaissance de l'une des six langues officielles de l'Union (anglais, arabe, chinois, espagnol, français, russe) au niveau avancé et connaissance d'une deuxième langue officielle au niveau intermédiaire. La connaissance d'une troisième langue officielle serait un avantage. (Selon les dispositions de la Résolution 626 du Conseil, l'assouplissement des conditions requises en matière de connaissances linguistiques peut être autorisé pour les candidats ressortissants de pays en développement: lorsque les candidats de ces pays possèdent une connaissance approfondie de l'une des langues officielles de l'Union, leur candidature pourra être prise en considération).

DROITS ET PRESTATIONS

Salaire:

Le traitement annuel total se compose d'un traitement annuel net (net d'impôts et avant déduction des contributions à l'assurance maladie et à la Caisse des pensions) en dollars USD et d'une indemnité de poste (indemnité de cherté de la vie). L'indemnité de poste est variable et peut être modifiée sans préavis, conformément aux taux fixés dans le régime commun des Nations Unies pour les traitements et les prestations.

Salaire annuel à partir de \$ 70,212 + indemnité de poste \$ 63,191

Les autres indemnités et prestations sont soumises aux conditions particulières de l'engagement, merci de vous référer à: [Ce que nous offrons](#)

INFORMATION SUR LE PROCESSUS DE RECRUTEMENT

Veuillez noter que tous les candidats doivent remplir une demande en ligne et fournir des informations complètes et exactes. Pour postuler, veuillez visiter le site Web de l'UIT carrières. L'évaluation des candidats est basée sur les critères de l'avis de vacance et peut inclure des tests et/ou des évaluations, ainsi qu'un entretien basé sur les compétences. L'UIT utilise des technologies de communication telles que la vidéo ou la téléconférence, la correspondance par e-mail, etc. pour l'évaluation des candidats. Veuillez noter que seuls les candidats sélectionnés seront contactés et que les candidats à l'étape de sélection finale seront soumis à une vérification des références sur la base des informations fournies. Les messages émanant d'adresses email différentes de celles de l'UIT - @itu.int - ne doivent en aucun cas être considérées. L'UIT ne facture aucun frais à aucun moment au cours du processus de recrutement.