NATO
NORTH ATLANTIC TREATY ORGANIZATION
INTERNATIONAL STAFF

OTAN
ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD
SECRÉTARIAT INTERNATIONAL

VACANCY NOTIFICATION/ NOTIFICATION DE LA VACANCE DU POSTE

Officer, Incident Management (2 posts) (241642)

Primary Location: Belgium-Brussels
NATO Body: NATO International Staff (NATO IS)
Schedule: Full-time
Application Deadline: 05-Jan-2025
Salary (Pay Basis): 7,540.44Euro (EUR) Monthly
Grade NATO Grade G17
Clearance Level NS
Description

Through this competition, NATO IS is aiming to Recruit for 2 positions:

- **Officer, Incident Management (G17)(OCIOxxxx) - Pending budget approval**
- **Officer, Incident Management (G17)(OCIO0013)**

1. SUMMARY

The NATO Chief Information Officer (CIO) function brings Information and Communications Technology (ICT) coherence across NATO Enterprise's civil and military bodies. The NATO CIO is empowered to realize the Allies' vision for the NATO Enterprise is accountable to the Secretary General and is responsible for the development of Enterprise directives and advice on the acquisition and use of information technologies and services. The NATO CIO provides Enterprise oversight on cybersecurity issues, and, in close coordination with all relevant NATO civil and military bodies, works towards the continual improvement of the cyber hygiene and cybersecurity posture in the NATO Enterprise.

The Office of the NATO CIO (OCIO) is an integrated staff organization comprised of International Staff (IS) and International Military Staff (IMS) members.

The Enterprise Security Branch (ESec) maintains Enterprise oversight on cybersecurity and enables awareness on specific risks, processes and incidents. It supports the NATO CIO in managing cybersecurity risks and incidents at Enterprise level, advises and supports the decision-making process for identifying the Enterprise risk appetite and risk acceptance for CIS Security.

The Branch executes functions deriving from the NATO CIO Enterprise risk owner and top-level incident manager roles for cybersecurity, coordinating incident response, business impact analysis, risk mitigation, mid- to long- term mitigation measures and lessons-identified definition. The Branch also maintains relations with key Enterprise military and civilian stakeholders at strategic, operational, tactical and technical levels.

The Security Processes Section (SPS) is responsible for ensuring correct support and representation in its role of Enterprise incident manager in front of multiple NATO relevant cyberspace stakeholders. The section is also responsible to provide liaison to network security, threats analysis and advanced technical operations in support of the defence of NATO-as-Enterprise Networks, services and capabilities.

The incumbent works within the Security Processes section and supports the coordination of the NATO Enterprise cyber incident management and response activities involving NATO enterprise CIS and services, in accordance with NATO's Cyber Incident Response Plan (CIRP). The incumbent supports the update and maintenance of the Enterprise Incident Management framework and related processes.

2. QUALIFICATIONS AND EXPERIENCE

ESSENTIAL

The incumbent must:

- hold a university degree, or an equivalent level of qualification, preferably in a cyber security related discipline;
- have at least 3 years of experience in cybersecurity, ideally in incident management and preferably in large civilian and/or international organization(s);
- demonstrate experience in the generation, provision and long-term assessment of cybersecurity recommendations and guidance originating from incidents happening in and through cyberspace;
- have knowledge and experience in coordinating multiple stakeholders' responses to cyber incidents in large, decentralized and multi-cultural organizations;
- have a good knowledge and experience in the cybersecurity domain and specifically in incident response processes;
- have working knowledge of network and infrastructure security principles, along with best practices for implementing protective measures, monitoring and logging;
- have experience in leading staff work on large and complex projects and to coordinate multiple stakeholders in different and separate locations;
- have a good knowledge of the principles, policy and procedures governing cyber defence;
- have the ability to draft clear and concise reports, produce and maintain security and risks logs and databases in support of security activities;
- be flexible and willing to work outside of normal office hours, during incident management activities, and travel when required;
- possess the following minimum levels of NATO's official languages (English/French): V ("Advanced") in one; I ("Beginner") in the other.

DESIRABLE

The following are considered an advantage:

- cybersecurity certifications such as CISSP, CCSP, CISM or equivalent post-graduate degree in cybersecurity;
- experience with NATO's cybersecurity environment, specifically in the CIS security field and related functions;
- understanding of the NATO organisation, its security policy and supporting directives.

3. MAIN ACCOUNTABILITIES

Policy Development
Contribute to the development of policy, directive and guidance documents in the OCIO areas of responsibility as per the incumbent's area of expertise. Provide advice to the Section Head on NATO enterprise incident management processes and procedures. Provide incident management advice and guidance to NATO Nations, NATO civil and military bodies and partner nations and international organizations. Develop high-level strategic documents and advice to improve enterprise incident management processes and procedures.

Expertise Development
Maintain and update an Enterprise-wide incident management framework to support the role of CIO as single point of authority for the Enterprise CIS. Based on the latest Security assessments and developments in cybersecurity threats, propose changes and improvements to the Framework, gathering ideas and lessons learned from other NATO experts across the Enterprise. Identify, develop and test new capabilities in support of Enterprise cyber incident management. Keep abreast with the latest technology developments in the incumbent's area of responsibilities and provide appropriate advice. Propose updates and improvements based on lessons identified from real life experience and from exercises.

Project Management
Support the definition of the section projects plan according to the OCIO role(s) in project management processes used in the NATO Enterprise. Identify main decision-makers and other stakeholders relevant for the project success, participate and contribute to project management boards as required. Maintain full understanding of project and program plans, identify and monitor project implementation risks, provide expertise and leadership in the resolution of exceptions and issues. Establish and maintain a network of relations with key project leaders in the NATO Enterprise, with a specific focus on ICT and Cybersecurity projects.

Planning and Execution
Coordinate and assess incident response activities involving Enterprise CIS and their effectiveness under pressure. Coordinate and develop mitigation and remediation actions in coordination with other members of the Risk Management Section in order to assure a coherent response Enterprise-wide to perceived threats and identified incidents.

Stakeholder Management
Establish and maintain a network of relations with key experts in the NATO Enterprise, with a specific focus on Enterprise-wide incident management. Develop close cooperation and working relationships with the NATO Operational community on the lifecycle of Enterprise security processes and practices, with a focus on incident management. Represent the Section at NATO and in various international settings, including in dialogues with government, civilian and military national representatives and giving presentations at conferences and seminars.

Knowledge Management
Draft background briefs, progress reports, prepare presentations, and other items for high-level meetings. Contribute to the information sharing with relevant NATO bodies and stakeholders (e.g. NATO Cyber Risk management Group (CRMG), the NATO Board of CISOA (BCISOA)) that contribute and support cyber incident management activities. On the basis of briefings, discussions and investigations, provide advice on evolving security programmes in NATO nations, NATO civilian and military bodies, and non-NATO entities.

Financial Management
Manage a predetermined budget for assigned projects.

4. INTERRELATIONSHIPS

The incumbent reports to the Head, Security Processes Section. The incumbent works in close cooperation with the OCIO members of staff, NATO Communications and Information Agency (NCIA), the Joint Intelligence and Security Division (JISD) the Cyberspace Operations Centre (CyOC), the NATO Cyber Risk Management Group (CRMG) and the NATO Board of CIS Operational Authorities (BCISOA) as well with experts of the various NATO Entities.

Direct reports: N/A
Indirect reports: N/A

5. COMPETENCIES

The incumbent must demonstrate:

- Analytical Thinking: Sees multiple relationships;
- Flexibility: Adapts to unforeseen situations;
- Impact and Influence: Takes multiple actions to persuade;
- Initiative: Is decisive in a time-sensitive situation;
- Organizational Awareness: Understands organisational climate and culture;
- Teamwork: Cooperates.

6. CONTRACT

Contract to be offered to the successful applicant (if non-seconded): Definite duration contract of three years; possibility of renewal for up to three years, during which the incumbent may apply for conversion to an indefinite duration contract.

Contract clause applicable:
In accordance with the contract policy, this is a post in which turnover is desirable for political reasons in order to be able to accommodate the Organisation's need to carry out its tasks as mandated by the Nations in a changing environment, for example by maintaining the flexibility necessary to shape the Organisation's skills profile, and to ensure appropriate international diversity.

The maximum period of service foreseen in this post is 6 years. The successful applicant will be offered a 3-year definite duration contract, which may be renewed for a further period of up to 3 years. However, according to the procedure described in the contract policy the incumbent may apply for conversion to an indefinite contract during the period of renewal and no later than one year before the end of contract.

If the successful applicant is seconded from the national administration of one of NATO's member States, a 3-year definite duration contract will be offered, which may be renewed for a further period of up to 3 years subject also to the agreement of the national authority concerned. The maximum period of service in the post as a seconded staff member is six years.

Serving staff will be offered a contract in accordance with the NATO Civilian Personnel Régulations.

7. USEFUL INFORMATION REGARDING APPLICATION AND RECRUITMENT PROCESS

Please note that we can only accept applications from nationals of NATO member countries. Applications must be submitted using e-recruitment system, as applicable:

- For NATO civilian staff members only: please apply via the internal recruitment portal (link);
- For all other applications: www.nato.int/recruitment

Before you apply to any position, we encourage you to click here and watch our video providing 6 tips to prepare you for your application and recruitment process.
Do you have questions on the application process in the system and not sure how to proceed? Click here for a video containing the information you need to successfully submit your application on time.

More information about the recruitment process and conditions of employment, can be found at our website (http://www.nato.int/cps/en/natolive/recruit-hq-e.htm)
Appointment will be subject to receipt of a **security clearance** (provided by the national Authorities of the selected candidate), approval of the candidate's **medical file** by the NATO Medical Adviser, verification of your study(ies) and work experience, and the successful completion of the **accreditation** and notification process by the relevant authorities.

NATO will not accept any phase of the recruitment and selection prepared, in whole or in part, by means of generative artificial-intelligence (AI) tools, including and without limitation to chatbots, such as Chat Generative Pre-trained Transformer (Chat GPT), or other language generating tools. NATO reserves the right to screen applications to identify the use of such tools. All applications prepared, in whole or in part, by means of such generative or creative AI applications may be rejected without further consideration at NATO's sole discretion, and NATO reserves the right to take further steps in such cases as appropriate.

8. ADDITIONAL INFORMATION

NATO is committed to diversity and inclusion, and strives to provide equal access to employment, advancement and retention, independent of gender, age, nationality, ethnic origin, religion or belief, cultural background, sexual orientation, and disability. NATO welcomes applications of nationals from all member Nations, and strongly encourages women to apply.

Building Integrity is a key element of NATO's core tasks. As an employer, NATO values commitment to the principles of integrity, transparency and accountability in accordance with international norms and practices established for the defence and related security sector. Selected candidates are expected to be role models of integrity, and to promote good governance through ongoing efforts in their work.

Due to the broad interest in NATO and the large number of potential candidates, telephone or e-mail enquiries cannot be dealt with.

Applicants who are not successful in this competition may be offered an appointment to another post of a similar nature, albeit at the same or a lower grade, provided they meet the necessary requirements.

The nature of this position may require the staff member at times to be called upon to travel for work and/or to work outside normal office hours.

The organization offers several work-life policies including Teleworking and Flexible Working arrangements (Flexitime) subject to business requirements.

Please note that the International Staff at NATO Headquarters in Brussels, Belgium is a non-smoking environment.

For information about the NATO Single Salary Scale (Grading, Allowances, etc.) please visit our website. Detailed data is available under the Salary and Benefits tab.

Administratrice/Administrateur (gestion des incidents) (2 postes) (241642)

Emplacement principal : Belgique-Bruxelles
Organisation : OTAN SI
Horaire : Temps plein
Date de retrait : 05-janv.-2025
Salaire (Base de paie) : 7 540,44Euro (EUR) Mensuelle
Grade NATO Grade G17
Niveau de l'habilitation de sécurité NS
Description

À travers ce concours, le Service International de l'OTANT cherche à recruter pour 2 positions :

- **Administratrice/Administrateur (gestion des incidents) (G17) (OCIOxxxx) - En attente d'approbation budgétaire**
- **Administratrice/Administrateur (gestion des incidents) (G17) (OCIO0013)**

1. RÉSUMÉ

La directrice/Le directeur des systèmes d'information (CIO) de l'OTAN assure la cohérence des technologies de l'information et de la communication (TIC) au sein des organismes civils et militaires de l'entreprise OTAN. Chargé(e) de concrétiser la vision des Alliés pour l'entreprise OTAN, elle/il rend compte à la/au secrétaire général(e) et est responsable, à l'échelle de l'entreprise, de l'élaboration des directives et de la formulation des avis concernant l'acquisition et l'utilisation des technologies de l'information et des services informatiques. Elle/Il assure la supervision des questions de cybersécurité à l'échelle de l'entreprise et, en étroite coordination avec tous les organismes civils et militaires de l'OTAN, s'emploie à améliorer constamment l'hygiène informatique et la posture de cybersécurité de l'entreprise.

Le Bureau de la/du CIO (OCIO) est une entité composite regroupant des membres du Secrétariat international (SI) et de l'État-major militaire international (EMI).

La Branche Sécurité des systèmes numériques d'entreprise (ESEC) supervise les questions de cybersécurité à l'échelle de l'entreprise OTAN et mène des actions de sensibilisation aux risques, processus et incidents spécifiques. Elle aide la/le CIO à gérer les risques et incidents de cybersécurité à l'échelle de l'entreprise OTAN, formule des avis et concourt au processus décisionnel lorsqu'il s'agit d'identifier le rapport au risque et le niveau de risque acceptable dans l'entreprise pour ce qui est de la sécurité des SIC. Elle exécute des fonctions découlant des rôles de propriétaire du risque et de principal gestionnaire des incidents en matière de cybersécurité pour l'entreprise OTAN qui incombent à la/au CIO ; elle coordonne ainsi la réponse aux incidents, les analyses d'incidences métier, l'atténuation des risques, les mesures d'atténuation à moyen et long terme et la définition des enseignements tirés. Elle entretient également des relations avec des parties prenantes civiles et militaires clés aux niveaux stratégique, opératif, tactique et technique.

La Section Processus de sécurité des systèmes numériques (SPS) a pour mission, en sa qualité de gestionnaire des incidents pour l'entreprise OTAN, d'assurer un soutien et une représentation corrects à divers acteurs OTAN du domaine cyber. Elle a également pour tâche d'assurer la liaison avec les entités responsables de la sécurité des réseaux, de l'analyse des menaces et des opérations techniques avancées à l'appui de la défense des réseaux, services et capacités de l'entreprise OTAN.

La/Le titulaire travaille au sein de la SPS et contribue à la coordination des activités de gestion et de réponse concernant les incidents cyber qui affectent les SIC et les services de l'entreprise OTAN, conformément au plan de réponse aux cyberincidents (CIRP) de l'Organisation. Elle/Il concourt à l'actualisation et à la maintenance du cadre pour la gestion des incidents de l'entreprise OTAN et des processus associés.

2. QUALIFICATIONS ET EXPÉRIENCE

ACQUIS ESSENTIELS

La/Le titulaire du poste doit :

- posséder un diplôme universitaire ou une qualification équivalente, de préférence dans un domaine lié à la cybersécurité ;
- avoir au moins trois ans d'expérience dans le domaine de la cybersécurité, idéalement dans la gestion des incidents, acquise de préférence au sein d'une ou de plusieurs organisations civiles et/ou internationales de grande envergure ;
- avoir une expérience avérée de la formulation, de la fourniture et de l'évaluation sur la durée de recommandations et d'orientations en matière de cybersécurité découlant d'incidents survenus dans le cyberespace et au travers de celui-ci ;
- avoir une connaissance théorique et pratique de la coordination des réponses de plusieurs intervenants face à un incident cyber dans une grande organisation multiculturelle décentralisée ;
- avoir une bonne connaissance théorique et pratique du domaine de la cybersécurité, et plus spécifiquement des processus de réponse aux incidents ;
- avoir une connaissance pratique des principes de la sécurité des réseaux et des infrastructures, ainsi que des bonnes pratiques en matière d'application de mesures de protection, de surveillance et de journalisation ;
- avoir déjà dirigé des équipes dans le cadre de grands projets complexes et assuré la coordination entre plusieurs intervenants travaillant sur des sites distincts ;
- avoir une bonne connaissance des principes, des politiques et des procédures qui régissent les activités de cyberdéfense ;
- être capable de rédiger des rapports clairs et concis ainsi que de produire et de tenir à jour des journaux et des bases de données concernant la sécurité et les risques, à l'appui d'activités relatives à la sécurité ;
- savoir faire preuve de flexibilité et être disposé(e) à travailler en dehors des heures normales de service, durant les activités de gestion des incidents, et à effectuer des déplacements lorsqu'il y a lieu.
- avoir au minimum le niveau de compétence V (« avancé ») dans l'une des deux langues officielles de l'OTAN (anglais/français), et le niveau I (« débutant ») dans l'autre ;

ACQUIS SOUHAITABLES

Seraient considérées comme autant d'atouts :

- des certifications en cybersécurité telles que CISSP, CCSP ou CISM, ou un diplôme de troisième cycle équivalent dans le domaine de la cybersécurité ;
- une expérience de l'environnement de cybersécurité de l'OTAN, en particulier dans des fonctions en lien avec la sécurité des SIC ou dans des fonctions connexes ;
- une connaissance de l'OTAN, de sa politique de sécurité et de ses directives complémentaires.

3. RESPONSABILITÉS PRINCIPALES

Élaboration des politiques
Contribue à l'élaboration de politiques, de directives et de documents d'orientation dans les domaines de responsabilité de l'OCIO qui relèvent de ses compétences. Donne à la/au chef de la Section des avis sur les processus et procédures de gestion des incidents à l'échelle de l'entreprise OTAN. Fournit aux pays de l'Alliance, aux organismes civils et militaires de l'OTAN, aux pays partenaires et à d'autres organisations internationales des avis et des orientations sur la gestion des incidents. Établit des documents stratégiques de haut niveau et formule des avis visant à améliorer les processus et les procédures de gestion des risques de l'entreprise OTAN.

Développement de l'expertise
Assure la maintenance et l'actualisation du cadre pour la gestion des incidents cyber à l'échelle de l'entreprise, apportant ainsi son concours à la/au CIO dans ses fonctions d'autorité unique pour les SIC de l'entreprise OTAN. Formule des propositions de modification et d'amélioration de ce cadre, sur la base des dernières évaluations de sécurité et de l'évolution des menaces cyber, en rassemblant à cet effet les idées et les enseignements provenant d'autres experts de l'entreprise OTAN. Recherche, développe et met à l'essai de nouvelles capacités à l'appui de la gestion des incidents cyber par l'entreprise OTAN. Se tient informé(e) de l'évolution des technologies dans son domaine de compétence et rend des avis éclairés. Propose des mises à jour et des améliorations sur la base des enseignements identifiés lors de situations réelles et d'exercices.

Gestion de projet
Contribue à la définition du plan de projets de la Section, dans le respect du/des rôles dévolus à l'OCIO dans les processus de gestion de projet utilisés au sein de l'entreprise OTAN. Identifie les principaux décideurs et autres intervenants nécessaires à la réussite des projets et, lorsqu'il y a lieu, participe et contribue aux travaux des comités de gestion de projet. Se tient parfaitement au fait des plans de projets et de programmes, identifie les risques pesant sur la mise en œuvre des projets et en assure le suivi, met son expertise et son leadership au service de la gestion des exceptions et de la résolution des problèmes. Instaure et entretient des relations de travail avec les principaux chefs de projet au sein de l'entreprise OTAN, en particulier pour les projets ayant trait aux TIC et à la cybersécurité.

Planification et exécution
Coordonne les activités de réponse aux incidents cyber affectant les SIC de l'entreprise OTAN et évalue leur efficacité dans les situations où la pression est importante. En concertation avec la Section Gestion des risques, élabore des mesures d'atténuation et de correction et coordonne leur mise en œuvre, l'objectif étant d'assurer une réponse cohérente, à l'échelle de l'entreprise, aux menaces perçues et aux incidents détectés.

Gestion des parties prenantes
Instaure et entretient des relations de travail avec les principaux experts au sein de l'entreprise OTAN, en particulier pour la gestion des incidents à l'échelle de l'entreprise. Entretient avec la communauté des opérations à l'OTAN une coopération et des relations de travail étroites pour ce qui est du cycle de vie des processus et des pratiques de sécurité d'entreprise, notamment de la gestion des incidents. Représente la Section au sein de l'OTAN et dans diverses instances internationales, notamment en prenant part aux dialogues avec les autorités nationales et les représentants civils et militaires des pays, et en faisant des exposés à des conférences et des séminaires.

Gestion des connaissances
Rédige des notes d'information et des rapports d'activité et prépare des exposés et d'autres supports pour des réunions de haut niveau. Contribue au partage de l'information avec les organismes et acteurs de l'OTAN qui concourent aux activités de gestion des incidents cyber (p. ex. Groupe de gestion du risque cyber (CRMG), Comité des autorités d'emploi des SIC (BCISOA)). À partir d'exposés, de débats et de recherches, formule des avis sur l'évolution des programmes de sécurité dans les pays membres et les organismes civils et militaires de l'OTAN ainsi que dans des entités non OTAN.

Gestion financière
Gère un budget prédéfini pour les projets qui lui sont confiés.

4. STRUCTURE ET LIAISONS

La/Le titulaire du poste relève de la/du chef de la Section Processus de sécurité des systèmes numériques. Elle/Il travaille en coopération étroite avec les membres de l'OCIO, l'Agence OTAN d'information et de communication (NCIA), la Division civilo-militaire Renseignement et sécurité (JIS), le Centre des cyberopérations (CyOC), le Groupe de gestion du risque cyber (CRMG) et le Comité des autorités d'emploi des SIC (BCISOA), ainsi qu'avec des experts des différentes entités OTAN.

Nombre de subordonné(e)s direct(e)s : sans objet
Nombre de subordonné(e)s indirect(e)s : sans objet

5. COMPÉTENCES

La/Le titulaire du poste doit faire preuve des compétences suivantes :

- Réflexion analytique : discerne les relations multiples.
- Flexibilité : s'adapte à des situations imprévues.
- Persuasion et influence : prend différentes mesures à des fins de persuasion.
- Initiative : fait preuve de décision dans les situations où il faut agir sans attendre.
- Compréhension organisationnelle : comprend le climat et la culture de l'Organisation.
- Travail en équipe : coopère.

6. CONTRAT

Contrat proposé (hors détachement) : contrat d'une durée déterminée de trois ans ; renouvelable pour une période de trois ans maximum, au cours de laquelle le/la titulaire pourra demander qu'il soit transformé en contrat de durée indéterminée.

Clause contractuelle applicable :
Conformément à la politique des contrats, il s'agit d'un poste auquel il est souhaitable, pour des raisons politiques, d'assurer une rotation de manière à pouvoir répondre au besoin qu'a l'Organisation d'exécuter les tâches qui lui sont confiées par les pays dans un environnement en constante évolution, notamment en préservant la souplesse nécessaire à l'adaptation de son profil de compétences, et de veiller au degré de diversité approprié à son caractère international.

La durée de service maximale prévue à ce poste est de six ans. La personne retenue se verra offrir un contrat d'une durée déterminée de trois ans, qui pourra être reconduit pour une période de trois ans maximum. Toutefois, conformément à la procédure décrite dans la politique des contrats, elle pourra demander, au plus tard un an avant l'expiration de la deuxième période, que son contrat soit transformé en contrat de durée indéterminée.

Si la personne retenue est détachée de l'administration d'un État membre de l'OTAN, elle se verra offrir un contrat d'une durée déterminée de trois ans, qui, sous réserve de l'accord des autorités nationales concernées, pourra être reconduit pour une période de trois ans maximum. À ce poste, la durée de service d'un agent détaché n'excède pas six ans.

Les agents en fonction se verront offrir un contrat conforme aux dispositions du Règlement du personnel civil de l'OTAN.

7. INFORMATIONS UTILES CONCERNANT LA PROCÉDURE DE CANDIDATURE ET DE RECRUTEMENT

On notera que seules les candidatures de ressortissant(e)s de pays de l'OTAN pourront être acceptées. Les candidatures doivent être soumises comme suit :

- pour les seuls agents civils de l'OTAN : via le portail de recrutement interne (lien) ;
- pour toutes les autres candidatures : via le lien www.nato.int/recruitment.

Il est recommandé de commencer par regarder ici une vidéo proposant six conseils destinés à aider les candidat(e)s à préparer leur dossier.

En outre, on trouvera ici une vidéo expliquant la marche à suivre sur le portail pour introduire son dossier de candidature et s'assurer de sa réception par l'OTAN dans les délais fixés.

On trouvera de plus amples informations concernant le processus de recrutement et les conditions d'emploi sur le site web de l'OTAN (http://www.nato.int/cps/fr/natolive/recruit-hq-e.htm).

La nomination se fera après vérification des diplômes et des antécédents professionnels de la/du candidat(e) retenu(e) et sous réserve de la délivrance d'une **habilitation de sécurité** par les autorités du pays dont la/le candidat(e) retenu(e) est ressortissant(e), de l'approbation de son **dossier médical** par la/le médecin-conseil de l'OTAN et de l'achèvement du processus d'**accréditation** et de notification par les autorités compétentes.

Dans le cadre de ses procédures de recrutement et de sélection, l'OTAN n'acceptera aucune réponse qui aura été produite, en tout ou en partie, au moyen d'un outil d'intelligence artificielle (IA) générative, notamment d'un modèle conversationnel comme ChatGPT (*Chat Generative Pre-trained Transformer*) ou de tout autre générateur de texte. L'Organisation se réserve le droit de vérifier si la/le candidat(e) a eu recours à de tels outils. Tout dossier de candidature élaboré, en tout ou en partie, à l'aide d'une application d'IA générative ou créative pourra être rejeté sans autre examen, à la seule discrétion de l'OTAN. Cette dernière se réserve également le droit de prendre toute autre mesure qu'elle jugerait nécessaire.

8. INFORMATIONS COMPLÉMENTAIRES

L'OTAN est déterminée à promouvoir la diversité et l'inclusion, et elle s'attache à assurer l'égalité de traitement en matière d'emploi, d'avancement et de fidélisation indépendamment de toute considération liée au genre, à l'âge, à la nationalité, à l'origine ethnique, à la religion ou aux croyances, à la culture, à l'orientation sexuelle, ou au handicap. L'Organisation examinera les candidatures de ressortissant(e)s de tous les pays membres, et encourage vivement les femmes à postuler.

Le développement de l'intégrité est un élément clé des tâches fondamentales de l'Alliance. En tant qu'employeur, l'OTAN attache une grande importance au respect des principes d'intégrité, de transparence et de redevabilité, conformément aux normes et aux pratiques internationales établies pour le secteur de la défense et de la sécurité s'y rapportant. Les candidat(e)s sélectionné(e)s doivent être des modèles d'intégrité et s'employer en permanence à promouvoir la bonne gouvernance dans le cadre de leur travail.

En raison du vif intérêt suscité par l'OTAN et du nombre élevé de candidatures potentielles, il ne pourra pas être donné suite aux demandes de renseignements adressées par téléphone ou par courrier électronique.

Les candidat(e)s qui ne seront pas retenu(e)s pour ce poste pourront se voir offrir un poste analogue, au même grade ou à un grade inférieur, pour autant qu'ils/elles remplissent les conditions requises.

De par la nature du poste, le/la titulaire peut parfois être amené(e) à voyager pour le travail et/ou à travailler en dehors des heures normales de service.

L'Organisation, en application de plusieurs politiques sur l'équilibre entre vie professionnelle et vie privée, propose notamment des possibilités de télétravail et d'horaire flexible sous réserve des exigences liées à la fonction.

Le Secrétariat international de l'OTAN est un environnement sans tabac.

Pour en savoir plus sur l’échelle unique de rémunération mise en place à l’OTAN (grades, indemnités, etc.), veuillez consulter notre site web. Des informations détaillées sont fournies sous l'onglet Salaires et allocations.