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

Head, Competency Center for Identity and Access Management Systems (IdAMS) (241414)

Primary Location: Belgium-Brussels
NATO Body: NATO International Staff (NATO IS)
Schedule: Full-time
Application Deadline: 13-Oct-2024
Salary (Pay Basis): 4,771.05Euro (EUR) Monthly
Grade: NATO Grade G11-G15
Clearance Level: CTS
Description:

'Pending budget approval'

1. SUMMARY

The Joint Intelligence and Security Division (JISD), under the leadership of the Assistant Secretary General (ASG) for Intelligence and Security, comprises two principal pillars: Intelligence, headed by the Deputy ASG for Intelligence; and the NATO Office of Security, (NOS) headed by the Deputy ASG for Security (DASG-S) / Director NOS.
The NOS is responsible for the overall coordination of NATO security member Nations, NATO civil and military bodies as well as International Organisations and partner. It is also responsible for the security of the NATO Headquarters (HQ) and its personnel in Brussels and abroad on mission and in satellite offices, and for the protection of the Secretary General. The NOS comprises the Office of the Director, the Security Policy Oversight Branch (SPOB), the Protective Security & Emergency Services Branch (PSESB), the Security Intelligence Branch (SIB) and the Close Protection Unit (CPU).
The PSESB's mission is to ensure the security and safety of the NATO Headquarters, its people, infrastructure and information. In coordination with the Host Nation, it analyses threats and vulnerabilities, determines risks and acts to minimize them. Its staff work in the following domains: access management; security regulations and infractions; physical security; security awareness and "special events" (high-level meetings at the NATO HQ and abroad). It also provides advice on protective security issues in the NATO satellite offices.

NATO Office of Security uses multiple systems to manage the identities and their access privileges in NATO HQ on a daily basis and also during the high-level events (Ministerial meetings and Summits).
IdAMS is the main identification system used at NATO HQ and is used as self-service for all users to request access to staff and experts coming to NATO HQ to work on a permanent basis or to attend official committees.

The incumbent leads the IDAMS Competency Center (IDAMS CC) and provides guidance and oversight over user aspects of design, development, implementation and operation of IdAMS and of the other different identity and access management solutions. They study and analyse current and emerging threats and vulnerabilities related to access management and subsequently determine and manage the risk, and formulate proposals to address and mitigate current and emerging risks and vulnerabilities. Under the direction of the NATO HQ Security Officer, the IDAMS CC functions as the NATO HQ central office for the administration of IdAMS and of the other identity and access management solutions. The incumbent will also represent NATO HQ Security Officer (HQ SO) in cross-functional teams, management boards and contractual negotiations.

2. QUALIFICATIONS AND EXPERIENCE

ESSENTIAL
The incumbent must:

- possess a university degree or equivalent certification ideally in fields of information technology, project management, systems engineering or other relevant field;
- have demonstrated experience of at least 3 years in the field of identity and access management systems, more specifically for large and complex buildings and sites;
- have managerial experience in leading small teams;
- possess substantial knowledge and understanding of physical and electronic security systems;
- possess proven experience in database management and be conversant with technical plans and document filing methodology;
- Combine strong analytical skills with the ability to prepare clear, precise and concise technical assessments and surveys as well as producing technical security reports;
- demonstrate drive for teamwork and good interpersonal communication skills;
- have the flexibility to work and travel outside of normal working hours in response to crises and urgent requirements;
- possess the following minimum levels in the official languages of NATO (English/French): V (“Advanced”) in one and III (“Intermediate”) in the other;

DESIRABLE

The following would be considered an advantage:

- more than 3 years of experience working with Automated Access Control Systems (AACS);
- more than 3 years of experience working on managing credentials for high level events;
- a good knowledge of NATO security policies and procedures and especially those related to protection of personal data, security zoning and access privileges of different categories based on the zoning;
- experience working effectively in a multi-national, multi-cultural organisation;
- experience as project manager for the implementation of ICT projects;
- knowledge of public procurement principles and procedures;
- experience in the implementation or management of self-service solutions and/or data and access privilege management.

3. MAIN ACCOUNTABILITIES

Expertise Development

Drive improvements in IDAMS processes and standards. Together with HQSO, the NATO Pass Office and the IT developers, ensure that the IDAMS components are operational and well understood across the NATO HQ. Organise and manage the requirements management process and control the requirements baseline. Organise and lead the user community in the implementation of new systems or system upgrades. Lead and coordinate the review of deliverables and operational testing processes. Ensure the accurate translation of business requirements into system functional and non-functional requirements. Contribute to, and coordinate as appropriate, initiatives aimed at transformation of processes and tools in the NATO identification and access management domain.

Information Management

Support implementation projects, typically involving the development and implementation of business processes to meet IDAMS' identified business needs, acquiring and utilising the necessary resources and skills within agreed parameters of cost, timescales, and quality. Manage issues relating to the integration of systems in the day-to-day work habits of NATO HQ stakeholders. Assist in evaluating IDAMS progress and contribute to issue resolution processes, taking corrective action as necessary and providing regular reporting to key stakeholders and the HQSO.

Knowledge Management

Analyse and document all or part of identity and access management systems in terms of business functions and processes based on the requirement from the NATO Office of Security and individual users. Define and document requirements for improving any aspect of the processes, systems and quantification of potential business and/or user benefits. Lead and control the development of user manuals, training materials, and

standard operating procedures. Implement and manage a suitable training program that properly weighs training needs and available resources.

People Management
Guide and oversee the work of the IDAMS CC team. Lead and manage the staff to build a well-respected, highly trained and motivated team. Provide regular feedback on performance. Support HQSO and the management team in implementing sound and inclusive management principles across PSESB. Recommend opportunities to improve staff performance, motivation, development and engagement. Encourage initiative, support creativity and the development and career aspirations of staff. Communicate on best practices, business processes, and systems-related aspects.

Project Management
Identify, analyse, design, and use resources efficiently and effectively. Review project performance of own projects as directed. Identify opportunities for improvement. Respond to changes in requirements in a positive and flexible manner, demonstrating resilience to change and uncertainty. Establish clear plans and timeframes for project implementation. Take responsibility for managing work projects to achieve results. See projects through to completion and identify lessons. Monitor project progress and adjust plans as required. Consider the risks, opportunities and ramifications of issues and longer-term impact of own work and work area. Assist in evaluating the different IDAMS's projects progress and contribute to issue resolution processes, taking corrective action as necessary and providing regular reporting to key stakeholder and the HQSO.

Stakeholder Management
Develop and maintain relationships with key stakeholders. Interface with the client base, the IDAMS and NATO Pass Office team, the system administrators, and NATO counterparts. Work in close collaboration with the NATO user community and lead and facilitate system requirements management processes. Participate, together with other System Authorities in the life-cycle management of HQSO Identification and Access Management systems. Represent HQSO interests in cross-functional teams, management boards, and contractual negotiations.
Perform any other related duty as assigned.

4. INTERRELATIONSHIPS

The Head Competency Center for Identity and Access Management (IdAMS) reports directly to the NATO HQ Security Officer. They work closely with the other NATO HQ stakeholders with members of the International Staff as well as members of Delegations, Missions, Military Representations and Agencies located on the NATO HQ compound.
Direct reports: 1
Indirect reports: 0

5. COMPETENCIES

The incumbent must demonstrate:

- Achievement: Works to meet standards.
- Analytical Thinking: Sees basic relationships.
- Clarity and Accuracy: Checks own work.
- Conceptual Thinking: Sees patterns based on life/work experience.
- Customer Service Orientation: Takes personal responsibility for correcting problems.
- Empathy: Reads non-verbal cues and understands meanings.
- Impact and Influence: Takes multiple actions to persuade.
- Initiative: Is decisive in a time-sensitive situation.
- 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.

NOTE: Irrespective of previous qualifications and experience, candidates for twin-graded posts will be appointed at the lower grade. Advancement to the higher grade is not automatic, and will not normally take place during the first three years of service in the post.

Under specific circumstances, serving staff members may be appointed directly to the higher grade, and a period of three years might be reduced by up to twenty four months for external candidates. These circumstances are described in the IS directive on twin-graded posts.

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.

Chef du Centre de compétence IdAMS (système de gestion des identités et des accès) (241414)

Emplacement principal : Belgique-Bruxelles
Organisation : OTAN SI
Horaire : Temps plein
Date de retrait : 13-oct.-2024
Salaire (Base de paie) : 4 771,05Euro (EUR) Mensuelle
Grade : NATO Grade G11-G15

Niveau de l'habilitation de sécurité : CTS

Description :

'En attente de l'approbation du budget'

1. RÉSUMÉ

La Division civilo-militaire Renseignement et sécurité (JISD), placée sous l'autorité de la/du secrétaire général(e) adjoint(e) (ASG) pour le renseignement et la sécurité, se compose de deux grands piliers : le pilier « renseignement », dirigé par la/le secrétaire général(e) adjoint(e) délégué(e) pour le renseignement (DASG/I), et le Bureau de sécurité de l'OTAN (NOS), dirigé par la/le secrétaire général(e) adjoint(e) délégué(e) pour la sécurité (DASG/S) et directrice/directeur du NOS.
Le NOS est responsable de la coordination générale de la sécurité à l'OTAN entre pays membres et organismes civils et militaires de l'OTAN, ainsi qu'avec les organisations internationales et les partenaires. Il est également chargé de la sécurité du siège de l'OTAN et de son personnel à Bruxelles et à l'étranger, en mission et dans les bureaux satellites, et de la protection de la/du secrétaire général(e). Le NOS comprend le Bureau de la directrice/du directeur, la Branche Supervision de la politique et de la sécurité (SPOB), la Branche Sécurité de protection et services de secours (PSESB), la Branche Renseignement de sécurité (SIB) et l'Équipe Protection rapprochée (CPU).
La PSESB a pour mission d'assurer la sécurité et la sûreté du siège de l'OTAN, de son personnel, de ses infrastructures et de ses informations. En coordination avec le pays hôte, elle analyse les menaces et les vulnérabilités, évalue les risques, puis prend des mesures visant à les réduire au minimum. Son personnel travaille dans les domaines suivants : gestion des accès, règlement et infractions de sécurité, sécurité physique, sensibilisation à la sécurité et « événements spéciaux » (réunions de haut niveau se tenant au siège de l'OTAN ou à l'étranger). Elle fournit en outre des avis aux bureaux satellites de l'OTAN sur les questions de sécurité de protection.
Le NOS recourt à divers systèmes pour gérer, au quotidien et pendant les événements de haut niveau (réunions ministérielles et sommets), les identités et les droits d'accès au siège de l'OTAN.

Le guichet électronique IdAMS est le principal système d'identification employé au siège de l'OTAN. C'est sur cette plateforme que les utilisateurs introduisent les demandes d'accès au siège, tant pour des agents venant y travailler à titre permanent que pour des experts venant participer à une réunion de comité.

En tant que chef du Centre de compétence IdAMS, la/le titulaire du poste oriente et supervise la conception, le développement, l'implémentation et le fonctionnement d'IdAMS et des autres solutions de gestion des identités et des accès, en se concentrant sur les aspects « utilisateurs ». Elle/Il étudie et analyse les vulnérabilités et les menaces liées à la gestion des accès, évalue et gère les risques qui en découlent et formule des propositions visant à traiter et atténuer les vulnérabilités et les menaces actuelles et émergentes. Le Centre de compétence IdAMS, placé sous l'autorité de l'officier de sécurité du siège, joue le rôle de bureau central du siège de l'OTAN pour l'administration de la plateforme IdAMS ainsi que des autres solutions de gestion des identités et des accès. La/Le titulaire du poste représente par ailleurs l'officier de sécurité du siège au sein d'équipes interfonctionnelles et de commissions de gestion, ainsi que dans le cadre de négociations contractuelles.

2. QUALIFICATIONS ET EXPÉRIENCE

ACQUIS ESSENTIELS

La/Le titulaire du poste doit :

- posséder un diplôme universitaire, ou une certification équivalente, idéalement dans les domaines des technologies de l'information, de la gestion de projet, de l'ingénierie systèmes ou dans une autre discipline présentant un intérêt pour le poste ;
- avoir une expérience avérée d'au moins trois ans dans le domaine des systèmes de gestion des identités et des accès, plus particulièrement acquise dans le contexte de grands bâtiments ou sites complexes ;
- avoir déjà géré et encadré de petites équipes ;
- avoir une connaissance et une compréhension approfondies des systèmes de sécurité physique et des systèmes de sécurité électroniques ;
- avoir une expérience avérée de la gestion de bases de données, être en mesure de lire des plans techniques et bien connaître les méthodes de classement de documents ;
- avoir d'excellentes capacités d'analyse, et être à même de produire des évaluations/études techniques claires, précises et concises ainsi que d'établir des rapports de sécurité techniques ;
- faire preuve d'un esprit d'équipe et avoir de bonnes compétences relationnelles en matière de communication ;
- être disposé(e) à voyager et à travailler en dehors des heures normales de service, en cas de crise ou d'urgence.
- avoir au minimum le niveau de compétence V (« avancé ») dans l'une des deux langues officielles de l'OTAN (anglais/français), et le niveau III (« intermédiaire ») dans l'autre.

ACQUIS SOUHAITABLES

Seraient considérées comme autant d'atouts :

- une expérience de plus de trois ans dans le domaine des systèmes de contrôle d'accès automatique (AACS) ;
- une expérience de plus de trois ans de la gestion des accréditations dans le cadre d'événements de haut niveau ;
- une bonne connaissance des politiques et des procédures de sécurité de l'OTAN, en particulier de celles qui concernent la protection des données à caractère personnel, le découpage en différentes zones de sécurité et les conditions d'accès à ces différentes zones;
- une expérience professionnelle concluante dans une organisation multinationale et multiculturelle ;
- une expérience de l'implémentation de solutions TIC (technologies de l'information et des communications) en tant que gestionnaire de projet ;
- une connaissance des principes et des procédures de passation des marchés publics ;
- une expérience de la mise en place ou de la gestion de solutions en libre-service ou de la gestion de données et de droits d'accès.

3. RESPONSABILITÉS PRINCIPALES

Développement de l'expertise

Pilote les travaux d'amélioration des processus et des normes IdAMS. En collaboration avec le Bureau Sécurité du siège, le Bureau des laissez-passer du siège et l'équipe de développeurs, veille à ce que les diverses composantes de la plateforme IdAMS soient opérationnelles et soient bien comprises dans l'ensemble du siège de l'OTAN. Organise et gère le processus de gestion des besoins et délimite les exigences de base. Accompagne la communauté des utilisateurs dans l'implémentation de nouveaux systèmes ou de mises à niveau des systèmes. Encadre et coordonne la revue des livrables et les processus de tests opérationnels. Veille à ce que les besoins métiers soient correctement transposés en spécifications système fonctionnelles ou non fonctionnelles. Contribue aux initiatives visant à modifier l'utilisation qui est faite à l'OTAN des processus et des outils de gestion des identités et des accès, et en assure la coordination s'il y a lieu.

Gestion de l'information

Apporte son concours aux projets d'implémentation, particulièrement aux projets de développement et d'implémentation des processus métiers destinés à répondre aux besoins métiers définis dans le cadre d'IdAMS, en acquérant et en utilisant les ressources et les compétences nécessaires, dans le respect des paramètres agréés

de coût, de calendrier et de qualité. Gère les difficultés relatives à l'intégration des systèmes dans les habitudes de travail des parties prenantes du siège de l'OTAN. Contribue à l'évaluation de l'état d'avancement d'IdAMS ainsi qu'aux processus de résolution des problèmes, en prenant les mesures correctrices nécessaires et en fournissant des rapports réguliers aux principales parties prenantes et au Bureau Sécurité du siège.

Gestion des connaissances

Analyse tout ou partie des systèmes de gestion des identités et des accès en examinant les fonctions et les processus métiers, sur la base des instructions du NOS et des besoins utilisateurs, et consigne les résultats de l'analyse. Définit et consigne les besoins s'agissant d'améliorer tout aspect d'un processus ou d'un système et de déterminer les avantages (métiers et/ou utilisateurs) pouvant être escomptés. Dirige et contrôle l'élaboration de manuels utilisateurs, de supports de formation et d'instructions permanentes. Met en place et gère un programme de formation assurant le juste équilibre entre besoins de formation et ressources disponibles.

Gestion des personnes

Encadre et supervise le travail des membres de l'équipe du Centre de compétence. Dirige et gère son personnel pour en faire une équipe hautement qualifiée et motivée, qui inspire le respect. Lui fournit régulièrement un retour sur ses performances. Prête son concours au Bureau Sécurité du siège et à l'équipe de gestion pour la mise en application de principes d'encadrement sains favorisant l'inclusivité à l'échelle de la PSESB. Met en avant les occasions d'améliorer les performances, la motivation et l'engagement de chacun(e) ainsi que les possibilités de développement professionnel. Encourage l'esprit d'initiative et la créativité et aide les agents à concrétiser leurs aspirations professionnelles. Communique au sujet des bonnes pratiques, des processus métiers et de différents éléments touchant aux systèmes.

Gestion de projet

Recense, analyse, conçoit et exploite les ressources avec efficacité et efficience. Évalue les résultats de ses propres projets, selon les instructions. Relève les éléments à améliorer. S'adapte à l'évolution des besoins de façon positive et souple, en faisant preuve de résilience face au changement et à l'incertitude. Élabore des

plans et des calendriers clairs pour la mise en œuvre des projets. S'engage personnellement dans la gestion des projets pour obtenir des résultats. Mène les projets à bonne fin et en tire des enseignements. Suit l'avancement des projets et adapte les plans selon les besoins. Réfléchit aux risques, aux opportunités et aux conséquences des problèmes, ainsi qu'aux incidences à plus long terme de son travail et de son domaine d'activité. Contribue à l'évaluation de l'état d'avancement des différents projets qui concernent IdAMS ainsi qu'aux processus de résolution des problèmes, en prenant les mesures correctrices nécessaires et en fournissant des rapports réguliers aux principales parties prenantes et au Bureau Sécurité du siège.

Gestion des parties prenantes

Noue et entretient des contacts avec les principales parties prenantes. Assure l'interface avec les clients, l'équipe IdAMS, le Bureau des laissez-passer du siège, les administratrices/administrateurs systèmes, ainsi qu'avec ses autres collègues au sein de l'OTAN. Travaille en étroite collaboration avec la communauté des utilisateurs OTAN, et dirige et facilite les processus de gestion des spécifications systèmes. Participe, avec les autres autorités responsables des systèmes, à la gestion du cycle de vie des systèmes de gestion des identités et des accès utilisés par le Bureau Sécurité du siège. Représente les intérêts du Bureau au sein d'équipes interfonctionnelles et de commissions de gestion, ainsi que dans le cadre de négociations contractuelles.

S'acquitte de toute autre tâche en rapport avec ses fonctions qui pourrait lui être confiée.

4. RELATIONS INTERPERSONNELLES

La/Le titulaire du poste relève directement de l'officier de sécurité du siège. Elle/Il est amené(e) à travailler en étroite collaboration avec les autres parties prenantes du siège, avec d'autres agents du Secrétariat international ainsi qu'avec des membres du personnel des délégations, des missions, des représentations militaires et des agences présentes sur le site.

Nombre de subordonné(e)s direct(e)s : 1

Nombre de subordonné(e)s indirect(e)s : 0

5. COMPÉTENCES

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

- Recherche de l'excellence : travaille dans le respect des normes.
- Réflexion analytique : discerne les relations élémentaires.
- Clarté et précision : vérifie son travail.
- Réflexion conceptuelle : discerne les constantes entre situations sur la base de l'expérience privée/professionnelle.
- Souci du service au client : s'engage personnellement à résoudre les problèmes.
- Empathie : détecte les indices non verbaux et en comprend la signification.
- 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.
- 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.

NOTE: Quelles que soient leurs qualifications et leur expérience, les candidat(e)s retenu(e)s pour un poste à grade jumelé sont nommé(e)s au grade le moins élevé. La promotion au grade le plus élevé n'est pas automatique et n'est en principe pas accordée au cours des trois premières années passées dans le poste.

Lorsque certaines conditions sont réunies, l'agent en fonction peut être nommé immédiatement au grade le plus élevé, et la période de trois ans peut être réduite, d'un maximum de vingt-quatre mois, pour les candidat(e)s externes. Ces conditions sont décrites dans la directive du Secrétariat international relative aux postes à grades jumelés.

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.