NATO Support and Procurement Agency (NSPA)

INFRASTRUCTURE, FACILITIES AND SUPPORT SERVICES DIVISION, Site Security Section

Junior Technician (Access Control and Systems Monitor)

Grade: 10:B4

Post No.: AF-61

Original:	English	|	*Clearance:*	SECRET
Date validated:	09 April 2026	|	*Duty Location:*	Capellen, LUX
Validated by:	A. Stoia	|	*Job Code:*	A64

SUMMARY

The incumbent reports to the Chief of Section (Site Security) and is responsible for acting as focal point for all Information Systems (IS) related matters related to the delivery of Infrastructure, Facilities and Support Services (IFSS), and the Automated and Visitor Access Control (AAC and VAC) Systems (ACSs) of the Capellen site. More precisely, the incumbent is responsible for executing the following tasks:

RESPONSIBILITIES

General Responsibilities

- Maintaining the IFSS and ACSs systems configurations according to NSPA defined Information Systems (IS) standards and priorities.
- Supporting applications for the delivery of the IFSS (such as Asset Tracking System, Building Management System, Fire Alarm System), and the ACSs.
- Supporting distributed computing IFSS and ACSs resources in accordance with NSPA procedures.
- Maintaining IFSS and ACSs inventory of configurations and ensuring their physical security.
- Maintaining IFSS and ACSs problem tracking system and determining equipment for servicing.
- Executing initial troubleshooting on the IFSS and ACSs hardware/software installed.
- Arranging receipt and return of material from/to designated storage locations.
- Customising, documenting and controlling end-user applications and other software as required.
- Collecting and coordinating requirements for the distributed IS planning and for the NSPA Information Systems Master Plan (NISMP).
- Installing new hardware and software in accordance with NSPA defined standards and procedures, NISMP and internal Service Level Agreement (SLA).
- Evaluating, in coordination with the IT Applications and SLA Division (IT), new hardware and software.
- Maintaining information and system security, restricting access to resources based on role and need, enabling access to system resources in accordance with the user profile for new users and disabling access at the users' departure or transfer and ensuring regulatory compliance.
- Managing role-based access control, least-privilege access, and segregation-of-duties models.
- Notifying the IT Division and network team, about all modifications to the physical network configuration.
- Assisting in the development and maintenance of visitor access and management procedures, including pre-registration and host approval workflows, identity verification and compliance checks, temporary badge and escort requirements.
- Assisting in the implementation of plans and procedures for safeguarding NATO classified information.
- Performing other functions as required in peacetime and any other appropriate functions assigned in times of crisis or war.
- In the event of crisis or war the incumbent will, subject to the agreement of their national authorities, remain in the service of the Agency.

Specific Responsibilities

- Interacting with IFSS and ACSs end-users and providing internal guidance for an efficient use of the equipment as well as internal tools [SAP, various internal and external SharePoint portals].
- Assisting in controlling, monitoring, operating and maintaining IS equipment including serviceability checks, control of back-up procedures, maintenance of hardware, software and data, reading, converting and importing data, and recording IS failures for internal and external customers.
- Creating, assigning, managing, and revoking access credentials and privileges for user, administrator, and service accounts to ensure appropriate access to enterprise assets and software.
- Establishing centralised access control to streamline user access and improve security.
- Monitoring access patterns and real-time adjusting permissions to address threats and organisational needs.
- Enabling real-time situational awareness, event correlation, and alert escalation.
- Applying NSPA and NATO Office of Security (NOS) security regulations, reporting any security incidents to the Section's Security Inspector, and assisting in resolving security violations.

QUALIFICATIONS

General Qualifications

- Higher vocational training in a relevant discipline and 2 years' post-related experience. Acceptable alternatives: secondary education and 4 years' post-related experience, or an equivalent education combined with an appropriate amount of relevant, professional experience.
- Formal training and experience in IS, IFSS and ACSs field with particular emphasis on end-user and workstation applications, problem solving, troubleshooting and direct end-user support.
- Demonstrated organisational and interpersonal skills to successfully work as a member of multinational/multi-disciplinary teams dealing with complex, interrelated technical issues.
- Well-developed communication skills (verbal and written) and the ability to make complex technical matters understood by various audiences.

Specific Qualifications

- Experience in giving guidance, assistance and training to end-users of IS systems – IFSS and ACSs.
- Demonstrated knowledge in the area of Information Technology (IT) [Networking, Internet technology, Interfacing systems, Operating System technology, Database Management Systems (DBMS), Systems security].

LANGUAGE QUALIFICATIONS

- NATO's official languages are English and French. Both languages are important in the work of this post, therefore fluency in one language and working knowledge of the other are essential.

DESIRABLE QUALIFICATIONS

- Good knowledge of NATO policy and directives governing security domains.

PERSONAL CHARACTERISTICS

- All NSPA personnel are expected to conduct themselves in accordance with the current NATO Code of Conduct agreed by the North Atlantic Council (NAC), and thus display the core values of integrity, impartiality, loyalty, accountability, and professionalism.

ADDITIONAL INFORMATION

- N/A

Agence OTAN de Soutien et d'Acquisition (NSPA)

DIVISION "INFRASTRUCTURES, INSTALLATIONS ET SERVICES DE SOUTIEN", Section "sécurité du site"

Technicien(ne) adjoint(e) [contrôle des accès et moniteur(-trice) des systèmes]

Grade : 10:B4

Poste n° : AF-61

Original :	Anglais	|	*Habilitation :*	SECRET
Date de validation :	9 avril 2026	|	*Lieu d'affectation :*	Capellen, LUX
Validé par :	A. Stoia	|	*Code poste :*	A64

RÉSUMÉ

Responsable envers le/la chef de section (sécurité du site), le/la titulaire est l'interlocuteur(-trice) privilégié(e) pour toutes les questions relatives aux systèmes d'information associés à la fourniture de services liés aux infrastructures, aux installations et au soutien (IFSS) ainsi qu'aux systèmes de contrôle d'accès automatique et de contrôle d'accès des visiteurs sur le site de Capellen. Il/Elle exécute plus précisément les tâches suivantes :

RESPONSABILITÉS

Responsabilités générales

- tenir à jour les configurations des systèmes IFSS et des systèmes de contrôle des accès, conformément aux normes et aux priorités définies par la NSPA en matière de systèmes d'information ;
- assurer le soutien des applications liées à la fourniture de services IFSS (comme les systèmes de suivi des biens corporels, de gestion de bâtiments et d'alarme incendie) et aux systèmes de contrôle des accès ;
- assurer le soutien des ressources informatiques réparties pour les systèmes IFSS et de contrôle des accès, conformément aux procédures de la NSPA ;
- tenir à jour l'inventaire des configurations des systèmes IFSS et de contrôle des accès, et veiller à leur sécurité physique ;
- tenir à jour un système de suivi des problèmes des systèmes IFSS et de contrôle des accès, et déterminer le matériel nécessaire pour la maintenance ;
- procéder au dépannage initial des matériels et logiciels installés pour les systèmes IFSS et de contrôle des accès ;
- prendre en charge les matériels et les remettre dans les emplacements de stockage prévus à cet effet ;
- adapter et contrôler les applications destinées aux utilisateurs finaux ainsi que les autres logiciels, selon les besoins, et établir la documentation correspondante ;
- recueillir et coordonner les besoins à prendre en compte pour la planification des systèmes d'information répartis et dans le Plan directeur des systèmes d'information de la NSPA (NISMP) ;
- installer les nouveaux matériels et logiciels conformément aux normes et procédures établies par la NSPA, au NISMP et à l'accord interne sur le niveau de service ;
- évaluer les nouveaux matériels et logiciels en coordination avec la Division "applications informatiques et accords sur le niveau de service" (IT) ;
- maintenir la sécurité des informations et des systèmes, restreindre l'accès aux ressources en fonction du rôle et du besoin, donner aux nouveaux utilisateurs les droits d'accès aux ressources des systèmes en fonction de leur profil d'utilisateur(-trice) et désactiver ces droits lors du départ ou du transfert des utilisateurs, et veiller à la conformité réglementaire ;
- gérer les modèles portant sur le contrôle d'accès basé sur les rôles, le droit d'accès minimal et la séparation des responsabilités ;
- informer la Division IT et l'équipe chargée du réseau de toutes les modifications apportées à la configuration physique du réseau ;
- aider à élaborer et à tenir à jour les procédures relatives à l'accès des visiteurs et à la gestion, ce qui comprend les flux de travail liés au préenregistrement et à l'approbation par la personne recevant le visiteur, les vérifications d'identité et les contrôles réglementaires, les exigences en matière de badge provisoire et d'accompagnement ;
- aider à la mise en œuvre des plans et procédures de protection des informations OTAN classifiées ;
- exercer d'autres fonctions selon les besoins en temps de paix et toute autre fonction appropriée qui lui sera confiée en période de crise ou en temps de guerre.
- En cas de crise ou de guerre, le/la titulaire restera au service de l'Agence, sous réserve de l'accord de ses autorités nationales.

Responsabilités particulières

- collaborer avec les utilisateurs finaux des systèmes IFSS et de contrôle des accès, et formuler des orientations en interne en vue d'une exploitation efficace du matériel ainsi que des outils internes (progiciel SAP et divers portails SharePoint internes et externes) ;
- aider à contrôler, à surveiller, à exploiter et à maintenir les matériels des systèmes d'information, c'est-à-dire effectuer notamment le contrôle de l'état de fonctionnement des matériels, le contrôle des procédures de sauvegarde et la maintenance des matériels et des logiciels, ainsi que la tenue à jour des données ; lire, convertir et importer des données et enregistrer les défaillances des systèmes d'information pour les clients internes et externes ;
- créer, attribuer, gérer et supprimer les identifiants et les privilèges d'accès concernant les comptes utilisateur, administrateur et services afin de garantir un accès approprié aux matériels et aux logiciels professionnels ;
- établir un contrôle centralisé des accès pour rationaliser l'accès des utilisateurs et améliorer la sécurité ;
- contrôler les schémas d'accès et ajuster les autorisations en temps réel afin de répondre aux menaces et aux besoins organisationnels ;
- faciliter la connaissance de la situation, la corrélation des événements et la remontée des alertes en temps réel ;
- appliquer les règlements de sécurité établie par la NSPA et le Bureau de sécurité de l'OTAN ; rendre compte de tout incident lié à la sécurité à l'inspecteur(-trice) de sécurité de la section et aider à régler les cas de violation des règles de sécurité.

QUALIFICATIONS

Qualifications générales

- Formation professionnelle supérieure dans une discipline pertinente assortie de deux ans d'expérience en lien avec le poste. Autres formations ou expérience acceptables : études secondaires assorties de quatre ans d'expérience en lien avec le poste, ou formation équivalente combinée à une expérience professionnelle suffisante et pertinente.
- Formation officielle et expérience dans le domaine des systèmes d'information, des systèmes IFSS et de contrôle des accès, particulièrement en ce qui concerne les applications destinées aux utilisateurs finaux et aux postes de travail, la résolution de problèmes, le dépannage et l'assistance directe aux utilisateurs finaux.
- Aptitudes confirmées dans le domaine de l'organisation et en matière de relations humaines, permettant de travailler avec succès en tant que membre d'équipes multinationales et pluridisciplinaires traitant de sujets techniques complexes et interdépendants.
- Très bonnes compétences en matière de communication (écrite et orale) et aptitude à faire en sorte que des questions techniques complexes soient comprises par des publics divers.

Qualifications particulières

- Expérience de la fourniture de conseils et d'assistance aux utilisateurs finaux des systèmes d'information (systèmes IFSS et de contrôle des accès) ainsi que de la formation de ces utilisateurs.
- Connaissances confirmées dans le domaine de l'informatique (réseautique, technologie Internet, systèmes en interface, technologie des systèmes d'exploitation, systèmes de gestion de base de données, sécurité des systèmes).

CONNAISSANCES LINGUISTIQUES

- Les langues officielles de l'OTAN sont l'anglais et le français. Les deux langues étant importantes pour le travail effectué à ce poste, il est essentiel d'avoir une bonne maîtrise de l'une et une connaissance pratique de l'autre.

QUALIFICATIONS SOUHAITABLES

- Bonne connaissance de la politique et des directives de l'OTAN régissant les domaines de la sécurité.

QUALITÉS PERSONNELLES

- Il est attendu de tous les membres du personnel de la NSPA qu'ils se comportent conformément au texte en vigueur du Code de conduite de l'OTAN adopté par le Conseil de l'Atlantique Nord et qu'en conséquence, ils incarnent les valeurs fondamentales que sont l'intégrité, l'impartialité, la loyauté, le sens des responsabilités et le professionnalisme.

INFORMATIONS COMPLÉMENTAIRES

- S.O.