JOB DESCRIPTION

Post Details:

Post Title:	**Principal Technician (ICT System)**	Organisational Element:	CSU Brussels
Military/Civilian:	Civilian	Location:	Brussels, BEL

Organisation context:

This is a position within the NATO Communications and Information Agency (NCIA), an organization of the North Atlantic Treaty Organization (NATO).

To strengthen the Alliance through connecting its forces, the NCIA delivers secure, coherent, cost effective and interoperable communications and information systems in support of consultation, command & control and enabling intelligence, surveillance and reconnaissance capabilities, for NATO, where and when required. It includes IT support to the Alliances' business processes (to include provision of IT shared services) to the NATO HQ, the Command Structure and NATO Agencies.

Organisational Element Statement of Functions:

NCIA CIS Support Unit (CSU) Brussels, located in Brussels (BEL) is the primary Information, Communications and Technology (ICT) service provider for 24/7 support to the Secretary General, the International Staff (IS), the International Military Staff (IMS) and other Customers in the NATO Headquarters in Brussels. CSU Brussels enables end-to-end CIS services and it installs, operates, maintains and supports the full range of CIS capabilities during peacetime, crisis and war throughout its allocated Area of Responsibility (AOR) and as otherwise directed.

Job role description:

A Principal Technician (ICT System) is responsible for installing, configuring, and maintaining computer hardware, software, and networks. He/she troubleshoot technical issues, provide technical support, and ensure that all systems are secure and up to date. He/she provide technical support to end-users and troubleshoot any issues that arise. They and may be involved in supporting the development of new ICT systems.

Duties and Responsibilities:

Software configuration

- Assists in designing, verifying, documenting, amending and refactoring moderately complex software configurations for deployment.
- Applies agreed standards and tools, to achieve a well-engineered result.
- Collaborates in reviews of work with others as appropriate.

System software

- Monitors operational systems for resource usage and failure rates, to inform and facilitate system software tuning.
- Applies system software parameters to maximise throughput and efficiency.
- Installs and tests new versions of system software.
- Contributes to preparation of software implementation procedures with fall back contingency plans.

Network support

- Contributes to the operational configuration of network components.
- Assists in the investigation and resolution of network problems.
- Assists with specified maintenance procedures.

Systems installation and removal

- Installs or removes system components using supplied installation instructions and tools.
- Conducts standard tests and contributes to investigations of problems and faults.
- Confirms the correct working of installations.
- Documents results in accordance with agreed procedures.

Release and deployment

- Uses approved tools and techniques for specific deployment activities.
- Administers the recording of activities, logging of results and documents technical activities undertaken.

Additional duties for this post:

- First and Second level fault resolution of Switching, Routing and other network Elements for all NATO HQ and remote sites supported networks;
- Fault diagnosing utilizing the CSU supported management platforms (e.g. Cisco ISE, Cisco CCC, Cisco NDFC, Zabbix...etc.);
- Ensure that Routing, Switching and other network elements are backed up;
- Liaise and collaborate internally, with the NCIA Service Lines and external providers for fault rectification and network improvement activities;
- Creation and maintenance of Standard Operating Procedures for Routing, Switching and other network systems;
- Propose and implement network improvements for QoS, Identity Services, Network response times and optimising network traffic flows;
- Review network and related design proposals;
- Adhere to ITIL standards and procedures;
- Resolve proactively potential network issues;
- Provide input to and assist with on-site security surveys;
- Perform assessments, provide documentation and coordinate security testing and verifications of network elements with CIS security;
- Liaise with support companies for reporting and follow-up of network incidents, upgrades;
- Obtain relevant network certification(s);

- Works with limited supervision;
- Maintains sound knowledge on implemented technologies;
- Advises his/her superiors and recommends technical solutions;
- Deputize for higher grade staff, if required;
- Perform other duties as may be required.

Education, Experience and Training (essential):

Education:

- Higher vocational training in a relevant discipline with 3 years post-related experience, or a secondary educational qualification with 5 years post-related experience.

Experience:

- Experience with support of CISCO Routing and Switching Elements;
- Experience with the configuration and operation of Network Fault, Configuration, Accounting, Performance and Security (FCAPS) Management systems;
- Experience with the support and implementation of network authentication and authorization systems and technologies (Cisco ISE, 802.1x, RADIUS, TACACS+);
- Experience with the support, implementation of Wireless network systems;
- Experience with the support and implementation of LAN technologies (e.g. HSRP, STP, Switching, VLANs, DHCP snooping, ARP Inspection, Port-Security);
- Experience with the support and implementation of Network Load Balancing techniques;
- Experience with the support of virtualised network systems;
- Very good knowledge and practical troubleshooting experience with communications protocols;
- Very good knowledge and experience with the support and implementation of DNS, and DHCP;
- Experience with network scripting;
- Experience with PKI certificates for network devices;
- Experience with preparing test plans, technical documentation and Standard Operating Procedures.

Training/ Certifications:

- The successful candidate must hold a valid Cisco Certified Network Professional (CCNP) certification or equivalent through extensive training with at least 5 years relevant professional experience;

Education, Experience and Training (desirable):

Education:

- Five years' experience in all aspects of maintenance, modification and operation of large complex multi-vendor IP communications networks and related equipment;
- Experience implementing and operating multi-tenancy network environments (VDC/VRF) and multicast network technologies;
- Knowledge of Datacentre virtualisation technologies;
- Knowledge of Firewall Technology and Concepts;
- Prior experience of working in an international environment comprising both military and civilian elements;
- Knowledge of NATO responsibilities and organization, including ACO and ACT;

Training/Certifications:

ITIL certification.

Behavioural competencies:

- *Delivering Results and Meeting Customer Expectations* - Focuses on customer needs and satisfaction; sets high standards for quality and quantity; monitors and maintains quality and productivity; works in a systematic, methodical and orderly way; consistently achieves project goals.
- *Adapting and Responding to Change* - Adapts to changing circumstances; tolerates ambiguity; accepts new ideas and change initiatives; adapts interpersonal style to suit different people or situations; shows an interest in new experiences.
- *Achieving Personal Work Goals and Objectives* - Accepts and tackles demanding goals with enthusiasm; works hard and puts in longer hours when it is necessary; seeks progression to roles of increased responsibility and influence; identifies own development needs and makes use of developmental or training opportunities

Language:	A thorough knowledge of one of the two NATO languages, both written and spoken, is essential and some knowledge of the other is desirable. **NOTE:** Most of the work of the NCIA is conducted in the English language.