IAMD COE JOB DESCRIPTION

PART I – JOB SPECIFICATIONS (REV2)

POST NUMBER:	**IAMD-FNS05**	DATE:	**SEP 2022**
HQ / UNIT:	**IAMD COE**	DUTY LOCATION:	**CHANIA/GR**
JOB TITLE:	**CIS Technician**	JOB CODE:	**FNS05**
NATIONALITY:	**GRC** SERVICE: **ANY**	AUTH.RANK:	**OF 1-2**

PART II – DUTIES

A. Post Context: This is a post in the Framework Nation Support Branch (FNSB) of the IAMD COE. The incumbent is responsible for providing technical services regarding the CIS Systems. The working language of the IAMD COE is English.

B. Reports to: The incumbent reports to the Head of FNS Branch.

C. Principal Duties:

1. Supports and maintains the CIS hardware such as routers, switches, PCs, laptops, tablets, cameras, microphones, headphones, speakers, general VTC equipment including screens and TVs, Voip Telephones ;
2. Acts as the Configuration control Manager for all CIS equipment;
3. Maintains the CIS servers properly and the relevant non break systems (e.g UPCs);
4. Maintains the wiring infrastructure such as Fiber optics, ethernet, sockets adaptors;
5. Prepares all the necessary equipment in order to support conferences, training, lessons and meetings with physical presence or virtually;
6. Acts as the Cryptographic Material Custodian;
   a. Controls and accounts for all Cryptographic material;
   b. Supports and maintains the Cryptographic material as required;

7. Analyses any reported suspicious cyber defence activity and decide whether it should be handled as an incident;

8. Executes cyber defence incident handling and response procedures when necessary;

9. Undertakes activities related with the identification, collection and preservation of digital information on security incidents;

10. Conducts cyber defence assessments on periodical basis to discover the vulnerabilities and exposures of CIS;

11. Conducts post-incident analysis activities, leveraging the information collected from the networks, to conduct root cause analysis and identify user

mistakes, unpatched vulnerabilities or potential gaps in preventive mechanisms that may have led to the incident;

12. Evaluates security information collected through long periods, to enable correlation and trends analysis, to be complemented with threat information in order to achieve cyberspace situational awareness;

13. Conducts security assessments on any software or hardware that is being evaluated for approval before deployment on the network;

14. Conducts periodical audits and inspections to verify that the cyber defence of the NATO related network is in compliance with the minimum requirements;

D. Additional Duties:

1. The incumbent of the post may be required to perform other specific duties as directed by the FNS Branch Head or higher.

PART III - QUALIFICATIONS

A. Essential Qualifications:

1. Professional/Experience:

a. Experience supporting and maintaining military telecommunications and information systems;

b. Extensive experience in Local Area Network (LAN) CIS support and maintenance;

c. Experience in Cryptographic material managing, control and usage.

2. Education/Training:

Completed National training on the support and maintenance of digital information systems, including routers, servers and workstations;

3. Security Clearance:

NATO SECRET. National authorities are to ensure that security clearance is provided before arrival of the individual at the IAMD COE.

4. Language (Listening, Speaking, Reading, Writing):

English: SLP 3333.

5. Standard Automated Information System (AIS) Knowledge:

a. Working knowledge of the current office suite (document, spreadsheet, presentation, database);

b. Working knowledge of the current mail tool;

c. Working knowledge of the Web Browsing tools.

B. Desirable Qualifications:

1. **Professional/Experience:**

a. Previous experience in NATO CIS.

b. Experience in dealing with large scale, modern CIS support management, network management, and operations and maintenance of IT systems;

c. Experience in CIS hardware and software configuration control and maintenance;

d. Extensive experience in server administration;

e. Experience in database management and programming;

f. Experience in staff duties, preferably in the field of office/CIS programming.

2. Education /Training:

a. NSO, Network Security Course M6-108, ACT 369.

b. NCIA, Oeiras, NATO CIS SECURITY OFFICER, A0280.

c. NCIA, MONS, Cyber Security Risk Assessment and Management. A3085.

d. NCIA, MONS, Endpoint Security and Network Access Control, A3049.

e. NCIA, MONS, Network Configuration and Troubleshooting, A3046.

f. NCIA, MONS, Computer Forensics Bootcamp, A3138.

g. NCIA, MONS, Firewall, Essentials: Configuration and Management, A3114

3. **Additional Language:**

Not Required.

C. Civilian Post:

Not Applicable.

D. Remarks:

1. A minimum handover period of two weeks is required on the rotation of appointees.