INTEGRATED AIR & MISSILE DEFENCE
CENTRE OF EXCELLENCE
Souda Air Base, 73100, Chania
https://www.iamd-coe.org

1st /2022 Steering Committee Meeting

POINT PAPER

Our Ref:	NU. 349	Tel.:	+302821440731
		NCN:	302-615-4031
Date:	1 Aug 2022	Email:	info@iamd-coe.org

TO: See Distribution

SUBJECT: **Job Descriptions CIS FNS04- & FNS05 update.**

No: **13**

PURPOSE: SC to be informed and approve the proposed amendment of the job Descriptions of post codes FNS04 (CIS Security Specialist) and FNS05 (CIS Technician) in order to fulfill the requirements of MC and ACT for Enhancing the protection of NATO related networks within NATO COEs.

BACKGROUND: Military Committee's (MC) decision on enhancing the protection of NATO Related Networks [enclosure 3] affected directly the operation and function of COEs requesting in coordination with the identified National Security Oversight Authority, to conduct an annual assessment to validate compliance with the ***Minimum Requirements of Cyber Defence for the Protection of NATO Related Networks*** (checklist included in the document/enclosure 1) and provide a signed written statement of compliance with the referenced minimum requirements to HQ SACT – CPD Branch.

This checklist, beyond any hardware or software improvements at the infrastructure of the CIS Systems of the CoEs, requested specific capabilities from designated person or team in order to execute best practice techniques, handling any incidents regarding cyber-Security, assessments of the threats etc.
In summary the requested capabilities are written below. In parenthesis the respective paragraph form the checklist is referred:

1. Analyses any reported suspicious cyber defence activity and decides whether it should be handled as an incident [2.1.4];

2. Executes cyber defence incident handling and response procedures when necessary [2.2.2];
3. Undertakes activities related with the identification, collection, and preservation of digital information on security incidents [2.2.4];
4. Conducts cyber defence assessments on a periodical basis to discover the vulnerabilities and exposures of CIS [3.2.1];
5. 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 [5.2.1];
6. 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 [5.3.1];
7. Conducts security assessments on any software or hardware that is being evaluated for approval before deployment on the network [3.2.2];
8. Conducts periodical audits and inspections to verify that the cyber defence of the NATO related network is in compliance with the minimum requirements [3.3.1];

ANALYSIS & STATUS: In this regard, the above capabilities should be assigned to the Team of IAMD CoE/Support Branch/ CIS section, post codes FNS04 &FNS05 and the relevant training if not accomplished to be amended as a desired qualification/training for the specific posts. The proposed training courses, either at NSO Oberammergau or NCIA, are oriented to the desired capabilities and customized for users like CoEs or other NATO entities.

Since March 2022, the IAMD COE, has adopted and implemented the Microsoft 365 Business Premium as the sophisticated, secure, working software platform with advanced cyberthreat protection and device management features. Microsoft 365 Business Premium suite is set up in that way, so the Minimum Requirements of Cyber Defence for the protection of NATO Related Networks are fully fulfilled.

The annual security assessment is planned to take place within 2022, in coordination with the Hellenic National Defence General Staffs respective National Security Accreditation Authority of Greece. Greece is IAMD COE's Framework Nation.

The National Security Accreditation Authority of the Hellenic National Defence General Staff is the same authority that grants the Security Accreditation and provides the Compliance Statement of IAMD CoE's NATO Secret LAN.

The following Job Description texts [Enclosure 1 & 2], address the requested changes for the respective amendment (updates/changes marked with red and strikethrough in black to the JDs).

FINANCIAL CONSIDERATIONS & FUNDING: Any financial impacts of the aforementioned changes will be covered from the existing budget of the current year (if needed) without the need for a supplementary budget. Any financial obligations for the next years will be foreseen in the shared budget of the respective Fiscal Years.

RECOMMENDATIONS & DECISION: The SC members are requested to approve the proposed changes as Enclosures 1 & 2.

FOR THE IAMD COE:

B. Gen (OF-6) Nikolaos KOKKONIS GRC (AF)
IAMD COE Director

ENCLOSURES

1. Draft JD, FNS04 CIS & Security Specialist Revision 2
2. Draft JD, FNS05 CIS Technician Revision 1
3. 2000/TSC-MVX-0010/TT-0452/NU_ENHANCING THE PROTECTION OF NATO RELATED NETWORKS WITHIN NATO COEs

DISTRIBUTION (via e-mail if not otherwise stated)

External

Action: IAMD COE SC - Members

Information: -

Internal

Action: FNS BRANCH

Information: DIRECTOR