Position Name: Cyber Security Officer (YPE)	**Employment Regime:** Seconded	
Ref. Number: ARM YPE 02*	**Location:** Yeghegnadzor	**Availability:** ASAP
Component/Department/Unit: Mission Support/CIS	**Security Clearance Level:** EU CONFIDENTIAL	**Open to Contributing Third States:** NO

1. Reporting Line

The Cyber Security Officer (YPE) reports to the Cyber Security Officer.

2. Main Tasks and Responsibilities:

- To facilitate and to assist the Cyber Security Officer in the implementation of Mission's cyber security controls;
- To assist to the Communication and Information Systems first-level support, initial troubleshooting for all directly reported issues and tickets assigned by the Help Desk and quickly restore the affected services;
- To administer and troubleshoot cloud, system, and network security solutions, updating software with latest security patches and ensuring the proper defences are present for each network and system resource;
- To identify, assess, and propose penetration tests and/or vulnerability assessment solutions and tools;
- To assist to the security systems configuration, analyse security requirements and recommend improvements;
- To monitor network traffic for suspicious behaviour, IT security metrics, SIEM and security logs, systems and service performance and security posture, providing periodic status reports;
- To research, evaluate, recommend, and introduce new IT security tools, techniques, services, and technologies to improve and innovate the Mission's IT security solutions portfolio;
- To support development and participate in the Mission's Cybersecurity Incident Response Team and work closely with stakeholders involved with Cybersecurity issues;
- To conduct regular technical IT security risk and control assessments/audits of systems and infrastructure, and provide actionable dashboards and data regarding status of remediation of security findings to vulnerability owners;
- To maintain the use of security tools (i.e. firewalls, data encryption, security certificates, IDS, IPS, SIEM) and services, to protect the Mission's data, electronic information, systems, and infrastructure.

3. General Tasks and Responsibilities:

- To identify and report on lessons learned and best practices within the respective area of responsibility;
- To contribute and ensure timely reporting on activities within the respective area of responsibility;
- To take account of gender equality and human rights aspects in the execution of tasks;
- To undertake any other related tasks as requested by the Line Manager(s);
- To support the appointed PoC for Cyber matters liaising with the CivOpsHQ.

4. Essential Qualifications and Experience:

- Successful completion of university studies of at least 3 years attested by a diploma in Computer Science, Information Systems or equivalent education OR a qualification in the National Qualifications Framework which is equivalent to level 6 in the European Qualifications Framework in Computer Science, Information Systems or equivalent education OR a qualification of the second cycle under the framework of qualifications of the European Higher Education Area, e.g. Bachelor's Degree;
  AND

- After having fulfilled the education requirements, a minimum of 2 years of relevant professional experience.

5. Essential Knowledge, Skills and Abilities:

- Knowledge of industry best practices in network, application, hardware and OS platform security and global security standards;
- Problem solving skills and the ability to understand and analyse complex technical end-users' problems and requests, and successfully manage and solve them daily;
- Ability to develop awareness campaigns;
- Ability to advise on security and counter intelligence;
- English language skills: minimum B2 (Independent User).

6. Desirable Qualifications and Experience:

- To possess current/valid professional industry certification(s), any one or more of CISSP, CISM, CISA, CRISC OR a combination of postgraduate certificates and certifications such as CompTIA Security+, CEH Certified Ethical Hacker, or GIAC certifications in cyber security or information security;
- Experience with Microsoft Windows/Linux server, Microsoft Active Directory and Group Policies, Microsoft 365 Security platform (i.e. Defender ATP), network routers and switches, next generation firewalls, data and drive encryption tools, and CA/PKI solutions;
- Professional experience in managing IT security and hands-on experience with related technologies, i.e. Firewalls, SIEM, IDS/IPS, NAC, MFA, Endpoint Security, and security hardening of networks, systems, and services;
- A combination of professional and relevant expertise and/or certifications in Microsoft, Cisco, Palo Alto, Vmware, EMC products and technologies;
- Familiarity with one or multiple ISO/IEC 27001, 27002 and 27005 Standards to help establishing a formal IT security governance and framework of operations, while also supporting in the system auditing processes;
- Background and familiarity with IT infrastructure methodologies, processes, and practices (i.e. ITSM/ ITIL);
- Experience with and/or good knowledge of modern security tools and products, including vulnerability scanners, analytical and testing tools (i.e. SPLUNK, MISP, Snort, Nessus, or similar);
- International experience, particularly in crisis areas with multi-national and international organisations.

7. Desirable Knowledge, Skills and Abilities:

- Knowledge of EU information security standards and formal accreditation processes;
- Knowledge of information system risks methodologies, cybersecurity frameworks (e.g. NIST or ISO 27000) and have good understanding of incidents investigation steps and processes;
- Project management skills and, possibly, practical experience with project management tools;
- Problem solving attitude and analytical ability to analyse complex IT systems configuration;
- Knowledge of information technology and security issues;
- Ability to develop and audit security systems using traceability framework;
- Knowledge of Russian and/or Armenian language(s).