Position Name: Cyber Security Officer	**Employment Regime:** Seconded	
Ref. Number: GEO AC 07	**Location:** Tbilisi	**Availability:** ASAP
Component/Department/Unit Mission Support Department/ CIS Section	**Level of Security Clearance:** EU SECRET	**Open to Contributing Third States:** No

1. **Reporting Line:**
   The Cyber Security Officer reports to the Head of Communication and Information Systems.

2. **Main Tasks and Responsibilities:**
   - To provide 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 install, 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.
   - Perform vulnerability and penetration tests, identifying and defending against threats, and developing disaster recovery plans.
   - To configure security systems, analyse security requirements and recommend improvements.
   - Monitor network traffic for suspicious behaviour, IT security metrics, SIEM and security logs, systems and service performance and security posture, providing periodic status reports.
   - Research, evaluate, recommend, and introduce new IT security tools, techniques, services, and technologies to improve and innovate the Mission's IT security solutions portfolio.
   - Support development and participate in the Mission's Cybersecurity Incident Response Team and work closely with stakeholders involved with Cybersecurity issues;
   - 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
   - Identify budgetary requirements, prepare requests for procurement proposals, draft technical specifications, and perform subsequent technical evaluation of received bids and commercial proposals in relation to IT Security products, solutions, and services.
   - Install, configure, and 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.
   - To prepare and provide training, advice and easy to follow user guidelines on using and maintaining IT and cyber security aspects.

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).

4. **Essential Qualifications and Experience:**
   - Successful completion of university studies of at least 3 years attested by a diploma, OR a qualification in the National Qualifications Framework which is equivalent to level 6 in the European Qualifications Framework, OR a qualification of the first cycle under the framework of qualifications of the European Higher Education Area, e.g. Bachelor's Degree OR equivalent and attested police or/and military education or training or an award of an equivalent rank; AND

- A minimum of 4 years of relevant professional experience, out of which a minimum of 2 years of experience in IT Security/Cyber Security area, after having fulfilled the education requirements.

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;
- Very good English Language skills.

6. Desirable Qualifications and Experience:

- 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;
- Involvement in establishing formal IT security governance and operations, and a familiarity with the support of audits and security certification. An ISO/IEC 27001 Lead Auditor certification would be beneficial;
- Background and familiarity with IT infrastructure methodologies, processes, and practices (i.e. ITSM/ ITIL);
- International experience, particular in crisis areas with multi-national and international organisations;
- 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).

7. Desirable Knowledge, Skills, and Abilities:

- Good knowledge of information system penetration techniques and risks, cybersecurity frameworks (e.g. NIST or ISO 27000) and have practical hands-on experience investigating and remediating active threats;
- Project management skills and practical experience with project management tools;
- Good knowledge of problem solving and analytical ability to analyse complex IT systems configuration;
- Knowledge of Russian and/or Georgian language(s).