Position: Mission Information Security Officer / Communication and Information Systems (CIS)	**Employment Regime:** Seconded/Contracted	**Post Category:** Mission Support Staff – Management Level (MSML)
Ref. number: GEO SE 12c	**Location:** Tbilisi	**Availability:** ASAP
Component/Department/Unit: Head of Mission Office / Security and Duty of Care Department	**Security Clearance Level:** EU SECRET	**Open to Contributing Third States:** No

1. Reporting Line:
The Mission Information Security Officer / Communication and Information Systems (CIS) reports to the Senior Mission Security Officer (SMSO).

2. Main Tasks and Responsibilities:

- To travel to all Mission areas including high risk areas as required;
- To act as the Mission focal point for information security compromise or suspicion of compromise;
- In collaboration with the Communications and Information Systems (CIS) Officer, the MISO operates in the following areas of activity:

Awareness Campaigns

- To develop and implement awareness campaigns and workshops related to information security systems (desk routine and passwords etc.), cyber security threats (phishing and hacking), personal operational security (use of social network and mobile phones) and classified information handling;

Classified Information Handling

- To develop Standard Operating Procedures (SOP) related to EU Policy and/or Council Security Regulations for EU staff;
- To audit permanently classified information systems;
- To track and maintain the Personal Security Clearance for EU Staff;
- To report security violations and compromised information matters;
- To develop and maintain any physical or technical structure for the protection of classified information.

Crypto Custodian

- To assume responsibilities as the Crypto Custodian for the Mission:
- To ensure registration, protection and transfer of accountable security items;
- To report to the EU Crypto Custodian (DGA5-SSICS) in case of security violation or security compromise;
- To develop and maintain a local framework for the use of crypto material, including audit and traceability;
- To liaise and maintain contact with EEAS for any topic in relation to crypto matters.

Information Security System (ISS)

- To develop the general framework for information security in cooperation with CIS including, organisational requirements, investigation capacities and incident reports;
- To provide input and assessment of existing and future IT infrastructure and application architecture from a security perspective;
- To participate in any study for implementation of new IT material, new interface (e.g. website);
- To ensure the monitoring of IT security systems including firewall etc.;
- To be responsible for investigative matters in relation to security violations;
- To participate in general ISS framework development and maintenance.

Cyber Security

- To participate in the general cyber-security framework development and deployment specifically related to threat intelligence and threat assessment;
- To develop an incident reporting line;
- To participate in investigations;
- To contribute to a good e-reputation.

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 at the level in the National Qualifications Framework 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, after having fulfilled the education requirements.

5. Essential Knowledge, Skills and Abilities:

- Knowledge of key information security principles and best practices,
- Knowledge of security management systems and programs;
- Ability to develop awareness campaigns;
- Ability to perform and analyse IT impact studies and implementing risk assessment recommendations;
- Ability to develop and audit security systems;

6. Desirable Qualifications and Experience:

- Experience in developing information security programs;
- Certification such as Certified Information Systems Security Professional (CISSP), forensic or malware analysis certification;
- Experience coordinating security-engineering projects and implementing systems;
- International experience, particularly in crisis areas with multinational and international organisations.

7. Desirable Knowledge, Skills and Abilities:

- Knowledge of EU information security standards and formal accreditation processes;
- Knowledge of information technology and security issues;
- Knowledge of Russian and/or Georgian language(s).