Job Description Print Report

Print Date: 2023-10-05 17:35:31

Position Review

Position Number	132619	Position Type	CFE/JPO	Subject to Radiation	No	Subject to GD	No
Hyperion Position Number		Fund Type	EBR	Parent Position	009726|Group Leader (SGIS-SSG)|11		
Organization	SGIS-Safeguards Security Group	FTE	1	CCOG 1	1A05		
Grade	P4	Duty Station	Vienna, Austria	CCOG 2			
Classified Grade		Position Title	Systems Security Engineer	Proposed New Title			
Master Version	3	Master Status	Approved	Approval Date	01-JAN-18		
Position Version	1	Position Status	Not Initiated	Approval Date			

Job Description Review

Organization Settings

The Department of Safeguards carries out the IAEA's duties and responsibilities as the world's nuclear inspectorate, supporting global efforts to stop the spread of nuclear weapons. The primary role of the Department is to develop and implement IAEA safeguards to ensure that there is no diversion of declared nuclear material from peaceful activities and no indications of undeclared nuclear material or activities in a State as a whole.

The Department comprises nuclear safeguards inspectors, responsible for carrying out inspections and verifications of all-safeguards relevant information for nuclear facilities in over 180 States; and technical staff responsible for a wide range of activities including: developing concepts and approaches for implementing safeguards; developing and maintaining safeguards equipment; providing analytical and laboratory services for sample analysis; collecting, evaluating and analyzing safeguards-relevant information; providing information and communication technology infrastructure and services; and providing programme coordination support.

The Office of Information and Communication Systems (SGIS) is responsible for the provision of secure Information and Communication Technology (ICT) services that enable the Department of Safeguards to deliver on its mandate. Major services provided by SGIS include provision of information technology project management services; development and maintenance of specialized ICT solutions; operation of resilient ICT infrastructure; provision of customer support services; and protection of safeguards information. In partnership with other organizational entities, SGIS is responsible for planning and implementing ICT strategies as well as promoting ICT standards.

Main Purpose

Reporting to the Safeguards IT Security Group Leader, the Systems Security Engineer ensures that: safeguards data and systems are adequately secured against relevant threats; information security risks associated with infrastructure and implementation decisions are known beforehand, so that mitigation strategies can be addressed; vulnerabilities are identified and managed appropriately; sensitive operations relevant to information security are captured and auditable; and Security projects are properly managed and delivered.

Role

The Systems Security Engineer plays several important roles within the Department of Safeguards and he/she is: (1) an incident responder, investigator and forensic analyst; (2) a custodian, architect and developer of the security event management system; (3) a reference point of the Department's forensic service; (4) a vulnerability expert, ensuring scanning and mitigation activities are performed in a timely manner; and (5) a general information security expert performing risk assessments and providing expert guidance as needed to management and project teams.

Partnership

The Systems Security Engineer collaborates extensively with the Safeguards Security Group, Information Systems Team and Software Development Teams, project managers and senior management on IT security matters. He/she liaises with external vendors and product suppliers on new information and technical specifications to evaluate and assess the suitability of their products.

Functions / Key results Expected

The Systems Security Engineer is expected to perform the following duties:

- Identify, investigate, lead and develop procedures for IT security incidents.
- Develop and advise on IT security standards and procedures which protect the Department's information assets.
- Develop and document IT security procedures aimed at enforcing policy while enabling the business needs of the Department.
- Provide IT forensics expertise to the Department of Safeguards and occasionally other departments in the Agency including the acquisition, preservation, authentication, examination and documentation of electronic evidence from a variety of media and systems.
- Contribute as a key player to ensuring the confidentiality, integrity and availability of Safeguards information systems and data through end-to-end IT security measures and by implementing appropriate technology and processes.
- Formulate, plan and execute IT security projects.
- Formulate and articulate expert opinions based on analysis.
- Conduct audits of Safeguards IT systems to ensure compliance with Safeguards security standards.
- Devise and initiate vulnerability scans and penetration tests with well-defined scope and actionable reports in order to improve the security of Safeguards IT systems.
- Produce high-quality oral and written reports, presenting complex technical matters clearly and concisely.
- Develop and manage the Department's IT event management system and perform auditing as needed to ensure appropriate access to resources is in place and to verify that policies and procedures are followed.
- Maintain proficiency in industry standard tools and practices and in IAEA policies and procedures
- Provide user/customer training on security awareness and related topics.
- Ensure that action is taken in a timely manner pursuant to the recommendations of periodic security audits, vulnerability assessments and threat and risk assessments.

Competencies

Core Competencies

Competency	Occupational Role	Definition
Communication	Individual Contributor	Communicates orally and in writing in a clear, concise and impartial manner. Takes time to listen to and

		understand the perspectives of others and proposes solutions.
Achieving Results	Individual Contributor	Takes initiative in defining realistic outputs and clarifying roles, responsibilities and expected results in the context of the Department/Division's programme. Evaluates his/her results realistically, drawing conclusions from lessons learned.
Teamwork	Individual Contributor	Actively contributes to achieving team results. Supports team decisions.
Planning and Organizing	Individual Contributor	Plans and organizes his/her own work in support of achieving the team or Section's priorities. Takes into account potential changes and proposes contingency plans.

Functional Competencies		
Competency	Occupational Role	Definition
Client orientation	Specialist	Helps clients to analyze their needs. Seeks to understand service needs from the client's perspective and ensure that the client's standards are met.
Commitment to continuous process improvement	Specialist	Plans and executes activities in the context of quality and risk management and identifies opportunities for process, system and structural improvement, as well as improving current practices. Analyses processes and procedures, and proposes improvements.
Technical/scientific credibility	Specialist	Ensures that work is in compliance with internationally accepted professional standards and scientific methods. Provides scientifically/technically accepted information that is credible and reliable.

Expertise		
Expertise	Description	Asset
Information Technology | IT Security	Thorough knowledge of Windows operating systems and security features including active directory, group policy and authentication methods.	N

Languages	
Languages	Asset Languages
English	Arabic Chinese French Russian Spanish

Qualification	
Qualification Title	Description
Master's Degree	Advanced university degree in information technology security, computer science, or engineering.
Bachelor's Degree	A first level university degree in information technology security, computer science, or engineering plus three years of relevant experience may be accepted in lieu of an advanced degree.
Other	Professional security certifications such as CISSP, CISA, and GIAC an asset.

Experience

A minimum of seven years of practical work experience in IT security.
Demonstrated experience in the following:
-Conducting forensic acquisitions and examinations for a variety of platforms, operating systems and file systems, including Windows (FAT & NTFS), Macintosh (HFS+), Linux (EXT2/3); and hands-on experience in forensic tools;
-Installation, management and development of an enterprise security event management system such as ArcSight
-Managing security incidents, analysis and reporting;
-Managing and running security-related projects;
-Formulating, developing and implementing IT security policies and procedures;
-Producing training materials and delivering training courses.
Experience with network security and analysis tools such as WireShark, tcpdump, Nessus, Metaspoit, and nmap.

Job Description Remarks

Requisition

Contract Type		Expected Start Date		Duration		Mobility	
Fully Competitive Recruitment			Travel				