IAEA International Atomic Energy Agency

Welcome. You are not signed in.

Job Description

Unit Head (IT Security Infrastructure)(P4) - (2018/0161 (013998))

Organization: MTIT-Security Systems Unit

Primary Location: Austria-Vienna-Vienna-IAEA Headquarters

Job Posting: 2018-03-09, 9:19:38 AM

Closing Date: 2018-04-23, 10:59:00 PM

Duration in Months: 36

Contract Type: Fixed Term - Regular

Probation Period: 1 Year

Organizational Setting

The Division of Information Technology provides support to the IAEA in the field of information and communication technology (ICT), including information systems for technical programmes and management. It is responsible for planning, developing and implementing an ICT strategy, for setting and enforcing common ICT standards throughout the Secretariat and for managing central ICT services. The IAEA's ICT infrastructure comprises hardware and software platforms, and cloud and externally-hosted services. The Division has implemented an IT service management model based on ITIL (IT Infrastructure Library) and Prince2 (Projects in a Controlled Environment) best practices.
The Infrastructure Services Section (ISS) is responsible for implementing, maintaining, and administering the ICT systems and services for high availability; designing, implementing, and operating IT security services; and managing the data centre. The platforms include Microsoft Windows servers, Linux servers, Oracle EBS infrastructure, data storage, and transmission networks, serving more than 2500 staff, as well as over 10000 external users around the world. The Section includes three Units: Network and Telecommunications, Enterprise Systems, and Security Systems.

Main Purpose

As a member of the ISS management team led by the Section Head, the Security Systems Unit (SSU) Head manages a team of ICT security engineers. He/she is responsible for engineering and administering central IT security systems, and integrating and holistically reviewing IT security across all systems on the network. He/she provides technical leadership, resource management and management of projects. The incumbent applies professional expertise on IT security (e.g. threat analysis, vulnerability management). He/she documents, manages and optimises operational security processes such as vulnerability management, security incident monitoring and security assessments. He/she advises on planning, design and implementation of protection, detection and forensic systems. He/she manages and coordinates the resolution of IT security incidents. Furthermore, he/she is responsible for sustaining service support measures and controls to ensure the resilience, performance, capacity and crisis recovery of those systems to meet the requirements of the organization.

Role

The SSU Head performs the roles of supervisor; security, monitoring and forensic expert; and project manager.

Functions / Key Results Expected

- Leadership: provide SSU with a clear direction, define priorities, delegate work and motivate staff.
- Planning: support the Section Head in developing and implementing annual work and resource plans. Assess their applicability within the overall Business-Technology Strategic Plan. Recognize and actively seek ways to secure the Agency's IT assets and services.
- Security Management: provide guidance by delivering a high-level IT security roadmap based on ISO 27002; develop, propose, recommend, and implement security solutions; document procedures and assure compliance; implement technical control mechanisms; assess and integrate IT security controls for the entire network; and perform security assessments, forensic analysis and vulnerability testing, and make recommendations for corrective actions.
- Service Management: take overall responsibility for ensuring the resilience, performance and security of services within agreed service levels.
- Project Management: plan, monitor and control projects using the PRINCE2 methodology.
- Problem Solving: investigate and resolve problems for services within his/her own area of responsibility, delegate to team members as appropriate, following ITIL processes, and manage major incidents through their lifecycle.

Competencies and Expertise

Core Competencies

Name	Definition
Planning and Organizing	Sets clearly defined objectives for himself/herself and the team or Section. Identifies and organizes deployment of resources based on assessed needs, taking into account possible changing circumstances. Monitors team's performance in meeting the assigned deadlines and milestones.
Communication	Encourages open communication and builds consensus. Uses tact and discretion in dealing with sensitive information, and keeps staff informed of decisions and directives as appropriate.
Achieving Results	Sets realistic targets for himself/herself and for the team; ensures availability of resources and supports staff members in achieving results. Monitors progress and performance; evaluates achievements and integrates lessons learned.
Teamwork	Encourages teamwork, builds effective teams and resolves problems by creating a supportive and collaborative team spirit, remaining mindful of the need to collaborate with people outside the immediate area of responsibility.

Functional Competencies

Name	Definition
Client orientation	Examines client plans and develops services and options to support ongoing relationships. Develops solutions that add value to the Agency's programmes and operations.
Commitment to continuous process improvement	Assesses the effectiveness of functions and systems as well as current practices; streamlines standards and processes and develops innovative approaches to programme development and implementation.
Technical/scientific credibility	Provides guidance and advice in his/her area of expertise on the application of scientific/professional methods, procedures and approaches.

Required Expertise

Function	Name	Expertise Description

Information Technology	IT Security	Strong knowledge of IT Security. Experience in establishing, implementing and maintaining of IT Security Systems.
Information Technology	Information Security and Risk Management	Strong knowledge and experience in Information Security, Threat Analysis and Risk Management.
Information Technology	Project Management	Experience in managing large and complex IT Security related projects following Project Management methodology such as PMP and Prince2.

Qualifications, Experience and Language skills

- Advanced university degree (or university degree and equivalent working experience) in Computer Science, Information Systems, Business Administration or a related field;
- Accredited Certification in Project Management such as PMP or Prince2 is desirable.
- Accredited Certification in IT Security and/or Information Security such as CISSP or equivalent
- Minimum of seven years of professional experience as a systems and/or security engineer in a large and complex IT enterprise environment (500+ servers). These should include five years of hands-on configuration, administration and troubleshooting experience.
- Extensive experience with security protection systems, tools and techniques (e.g. firewalls, proxies, IDS).
- Extensive experience with security detection systems, tools and techniques (e.g. ArcSight, Nessus).
- Extensive experience in information security methodologies, including threat analysis, vulnerability management and security assessments.
- Experience in managing a team of highly specialized IT staff.
- Experience in information security forensic concept and tools.
- Experience in IT service management (i.e. ITIL), supporting innovation and managing change.
- Extensive experience with procedure development, implementation, and compliance.
- Experience with ISO 27001 is preferred.
- Experience with cloud security.
- Experience with classified networks, information classification, and confidentiality requirements associated with high security environments.
- Excellent oral and written command of English. Knowledge of other official IAEA languages (Arabic, Chinese, English, French, Russian and Spanish) is an asset.

Remuneration

The IAEA offers an attractive remuneration package including a tax-free annual net base salary starting at **US $71332** (subject to mandatory deductions for pension contributions and health insurance), a variable post adjustment which currently amounts to **US $ 38234***, dependency benefits, rental subsidy, education grant, relocation and repatriation expenses; 6 weeks' annual vacation, home leave, pension plan and health insurance

---

Applications from qualified women and candidates from developing countries are encouraged

Applicants should be aware that IAEA staff members are international civil servants and may not accept instructions from any other authority. The IAEA is committed to applying the highest ethical standards in carrying out its mandate. As part of the United Nations common system, the IAEA subscribes to the following core ethical standards (or values): Integrity, Professionalism and Respect for diversity. Staff members may be assigned to any location. The IAEA retains the discretion not to make any appointment to this vacancy, to make an appointment at a lower grade or with a different contract type, or to make an appointment with a modified job description or for shorter duration than indicated above. Testing may be part of the recruitment process

---

Apply Online | Add to My Job Cart | SHARE