

Institute of Public Administration

Job Description

Title of Post: Cyber and Information Security Manager

Grade: Grade 3

Reports to: Senior ICT & Support Services Manager.

Job Function: To lead out in the management, governance, enhancement, auditing and securing of all ICT systems, information and data against internal and external threats.

The position holder will be responsible for the implementation, management and audit of policies and controls that underpin the cybersecurity function in the IPA. As a manager in this business critical position, the position holder is required to take ownership of, and ensure highest standards of good governance in the management of Information Security.

This role will have oversight of the cyber security element of the IPA business continuity solutions and other business critical components of the ICT infrastructure. The position holder will be responsible for scoping penetration-testing activities to identify security weaknesses within the IPAs technology environments.

The Cyber and Information Security Manager is required to assist in the development of Information Security Management Systems and align the IPA with ISO 27001 standards. The holder will also have responsibility for reviewing and assessing third party suppliers and contracts to assess associated risks and fit with policies and standards.

The Cyber and Information Security Manager will be required to:

- Lead in the design and implementation of standards, policies, guidelines and appropriate architectural principles to ensure the IPA cyber security goals and targets are met.
- Develop risk-based strategies in conjunction with the ICT plans for future system enhancements, in line with the overall IPA business model.
- Recognise potential opportunities for enhancing the IPA's security, ensuring minimal impact to the stakeholders and business delivery.
- Work closely with internal and external stakeholders including the IPA SMG, Senior ICT manager and the Data Protection Officer and to ensure that appropriate security guidance is provided, documented and implemented.
- Develop a culture of collaborative and in-depth understanding as to why security testing is required for both external and internal stakeholders.
- Provide quality reports to summarise test activities, including objectives, planning, methodologies, results, analyses and recommendations to both technical and non-technical audiences. From the output of the reports provide suggested approaches to enhance further solutions.

Main duties include:

- **Cyber Security**
 - Identifying IT Security risks and determining appropriate remedial actions.
 - Develop security strategies, policies, standards, and processes.
 - Oversight of vulnerability assessments and penetration testing.
 - Identity and Access Management solutions.
 - Lead on ICT Incident Response support and conduct investigations.
 - Contributing to team knowledge and capability development.
 - Perform regular audits to ensure security practices are compliant.
 - Provide support and troubleshooting services as part of the IT Support Team.
 - Deliver the specification, design, test and deployment of solutions.
- **Data Security Compliance**
 - Ensure compliance with all applicable data legislation/regulation including General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS).

Person Specification/experience:

- The Cyber and Information Security Manager should hold a third level ICT- related qualification (equivalent to level 7 on the NFQ)
- Demonstrable experience of working within the Cyber Security environment.
- A minimum of five years, hand-on, operational experience within an ICT environment.
- Possess at least one Cyber and Information Security relevant professional designation for example CISSP/SSCP/ CEH/ENCE/ACE/ OSCP/ Sec +.

Experience in some or all of the following is essential:

- Practical experience in applying Cyber Security frameworks.
- Broad knowledge of a wide range of Information Technology systems and a deep understanding of the inherent security risks associated with these technologies.
- Intrusion detection solutions.
- System monitoring.
- Network topology and security.
- Penetration testing.
- Back-up Systems, Firewall Security Software.

In addition, the following personal attributes are essential:

- Excellent interpersonal and analytical skills.
- Excellent management, organisational and problem solving skills, with high attention to detail.
- Possess exceptional communication skills, with the ability to build positive relationships with a variety of stakeholders in a multi-disciplinary environment.
- Demonstrable solid decision making abilities.
- Management and delivery of results.
- An enthusiastic approach to problem solving at all levels.
- Strong technical aptitude.
- An ability to work as part of a team.
- Dynamic, adaptable and flexible.
- Excellent knowledge of the technology market, information security, and cybersecurity.

General Conditions:

This is a permanent fulltime position.

The salary range for this position is €57,071 to €88,034 (14 points including two LSIs) per annum pro rata

How to apply

Please email your curriculum vitae together with a covering letter stating the title of the post applied for and how you meet the requirements to recruit@ipa.ie by 1pm, Friday 5 November 2021.