**Job Description**

**IT Security Officer**

**Role Profiles** RPITS004, RPITS005, RPITS013

**Service/Team** Information Technology & Programmes

**Reports to** IT Security Manager

**Responsible for** N/A

**Number of posts** 1

**Post number** 104026

**Job Purpose**

To provide ICT security support for a range of software and hardware platforms accessed on desk-based and mobile devices, ensuring the integrity, confidentiality, and availability of business applications, data networks, and server infrastructure. This role ensures that colleagues across the organisation operate within a secure IT environment, mitigating risks and responding to security incidents effectively.

This role will focus on handling and resolving escalated security incidents and escalating complex cases to the appropriate teams where necessary. As an experienced team member, the post holder will manage security cases, support project activities, and work closely with internal customers across the Council to promote security awareness.

**Key Responsibilities**

* Provide administrative support to key IT security applications and services, ensuring compliance with security policies and standards.
* Offer second and third-line security support services, escalating unresolved security incidents to third parties, colleagues or specific internal teams as needed.
* Investigate, diagnose, and resolve security issues across a variety of platforms and devices.
* Liaise with third-party vendors and service providers to ensure timely resolution of security incidents and compliance with service agreements.
* Assisting with regular security assessments, vulnerability scans, and audits to identify and mitigate potential risks.
* Support the business with changes to procedures and policies within key security solutions, ensuring alignment with regulatory requirements.
* Assist in the deployment and configuration of security controls across IT infrastructure, including firewalls, endpoint protection, and access controls.
* Monitor and analyse security logs and alerts to identify potential threats and take appropriate action.
* Understanding the function of a SIEM and SOC solution.
* Maintain accurate documentation of security incidents, configurations, and processes to support compliance and reporting.
* Communicate security-related information effectively to non-technical stakeholders, enabling them to understand and mitigate risks.
* Identify trends in security incidents and propose proactive solutions to enhance the organisation's security posture.
* Contribute to the development of security awareness training materials and user guides to promote a culture of cybersecurity within the organisation.
* Participate in ICT security projects, providing technical expertise and ensuring successful implementation while minimising disruption to business operations.
* Ensure compliance with data protection legislation and cybersecurity best practices to safeguard organisational information assets.

**Skills, Knowledge & Experience**

* ITIL Intermediate certification (or working towards it).
* Experience in providing ICT security support for hardware and software solutions.
* Comprehensive knowledge of ICT security protocols, processes, and procedures.
* Experience with Office applications and data storage solutions, such as SharePoint.
* Knowledge of security frameworks such as ISO 27001, NIST, and Cyber Essentials.
* Strong understanding of industry-standard security platforms and applications, including Microsoft 365 Security, Azure Security Centre, firewalls, and SIEM solutions.
* Up-to-date knowledge of current cybersecurity threats, trends, and mitigation strategies.
* Ability to assess security risks and recommend appropriate mitigation measures.
* Proficiency in translating technical security concepts into clear, accessible language for non-technical users.
* Excellent organisational and prioritisation skills to manage competing demands and deadlines.
* Strong analytical and problem-solving capabilities to diagnose and resolve a broad range of security incidents.

**Personal Qualities & Attributes**

* Highly organised with the ability to multitask effectively.
* Enthusiastic, self-motivated, and dedicated to ensuring a secure IT environment.
* Strong communication and interpersonal skills, with the ability to work independently and collaboratively.
* Attention to detail and a proactive approach to identifying and mitigating security risks.

**Job Requirements**

* A valid UK driving licence and have access to a vehicle would be beneficial or have viable alternative transport arrangements.
* Willingness to participate in an on-call rota and work outside normal business hours, including evenings and weekends, as required.
* Ability to handle sensitive security incidents with discretion and professionalism.
* Willingness to work in data centre environments with exposure to cold temperatures and noisy conditions.

**Working Conditions**

* The role may involve physical tasks such as installing and securing ICT equipment.
* The role requires time spent in data centre environments and exposure to equipment noise levels.
* Participation in a standby/call-out rota and potential overtime requirements, including weekends and evenings.