ROYAL
BALLET &
OPERA

JOB DESCRIPTION

Role / Title: **Cyber Security Engineer**

Reports to: **Cyber Security Manager**

Main Purpose of the Job

As a Cyber Security Engineer, you will be an essential part of our team, helping to design, develop, and enhance our cybersecurity capabilities. You will assist in selecting, implementing, and managing security tools and technologies, focusing on detecting, preventing, and analysing security threats. Your role will be crucial in supporting our efforts to protect the organisation's digital assets and ensure a secure environment for our operations.

Key Responsibilities

- Design, implement, and maintain security measures to protect computer systems, networks, and data at the Royal Ballet & Opera.
- Conduct regular security assessments and vulnerability testing.
- Assist in developing and enforcing security policies and procedures.
- Collaborate with the rest of IT and other departments to ensure security best practices are followed.
- Stay up to date with the latest security trends, threats, and technology solutions.
- Provide training and guidance to staff on security protocols.
- Monitor for security breaches, intrusions, and unauthorised activities.
- Evaluate and test security solutions.
- Investigate and respond to security alerts and incidents.
- Collaborate with stakeholders to address cybersecurity concerns and provide recommendations.
- Produce reports for technical and non-technical audiences.
- Assist with internal and external cybersecurity audits.

Role Proficiency

The role demands proficiency in several skills, each categorised into four ascending levels: Awareness, Working, Proficient, and Expert. Here are the primary skills and their corresponding levels for this role:

- **Security Technology (Level: Practitioner)** - Recognised for knowledge of systems and tools, understanding the implications of vulnerabilities on current and future systems, and acknowledged within the broader security industry.

- **Technical Understanding (Level: Practitioner) -** Understanding core Security technical concepts related to the role and applying them with guidance.

- **Research and Innovation (Level: Working)** - Contribute to security technology advancements, identify, and help integrate new technologies within the business, and engage with the wider security community.

- **Communication (Level: Working)** - Demonstrate an understanding of security concepts, explain security and risk to both technical and non-technical stakeholders, address challenges, manage stakeholder expectations, and adapt communications to achieve consensus.

- **Designing Secure Systems (Level: Awareness)** – Fundamental knowledge in designing and evaluating new systems.

- **Analysis (Level: Working)** – Assist with the analysis of technical solutions, assist with information collection and analysis, and provide input on policies and requirements.

- **Ownership and Initiative (Level: Awareness):** Taking responsibility for assigned issues until resolved or reassigned.

- **Asset and Configuration Management (Level: Working):** Help maintain secure, accurate configurations and control IT assets; verifying asset vulnerabilities and configuration.

- **Change Management (Level: Awareness):** Implementing changes based on requests and applying change control procedures.

PERSON SPECIFICATION

- Demonstrable interest, training, experience, or certifications in Information Security (such as Security+, CISSP, CEH or others), and associated industry best practices.
- Bachelor’s degree in computer science, Information Technology, or a related field (or equivalent demonstrable experience).
- Proven experience as a Cyber Security Engineer or similar role with a technical approach to Information Security.
- Familiarity with Azure, AWS, 365 Admin, MDM, Antivirus, Firewalls, Vulnerability scanners, and Penetration testing tools.
- Knowledge of programming and scripting languages (e.g., Python, PowerShell).
- Understanding of regulatory requirements and compliance (e.g., GDPR, Data Protection Act 2018).
- Problem-solving and analytical skills.
- Strong communication and teamwork abilities.
- Familiarity with security frameworks and standards (e.g., ISO 27001, NIST).

- Strong verbal and written communication skills, with the ability to adapt information delivery based on the target audience.

This Job Description reflects the current situation. It does not preclude change or development that might be required in the future.

disability confident EMPLOYER

employers network for equality and inclusion www.enei.org.uk Member

Stonewall DIVERSITY CHAMPION