**Job Description**

|  |  |
| --- | --- |
| **Post Title** | Principal Cyber Security and Infrastructure Specialist |
| **Directorate** | Digital and Data |
| **Reports to** | Technical Services Manager |
| **Direct Reports** | 0 permanent staff but responsible for contracted staff and contracts to deliver solutions  |
| **Salary Band** | 40-44 (6-months pro-rata) |
| **Key Relationships** | Principal Cyber Security & Infrastructure Specialist and Security & Information Risk Adviser |

**Role Purpose**

The role will be responsible for leading, managing, developing, and maintaining the organisation’s operational cyber security infrastructure and systems. Ensuring a compliant approach which is aligned with best practice and the Digital and Data strategy. You will work across the Digital and Data department and wider business, being the primary person for all operational cyber security requirements, advice, and support. You will be the expert on all things under this SME umbrella, transforming the Digital and Data services from legacy systems to modern secure platforms. To support critical Digital and Data systems out of normal business hours. Enabling the business to continually develop and improve its Digital and Data platforms.

**Responsibilities**

* Manage, maintain and report on the WMCA’s operational cyber security systems, assessing and prioritising up-to-date cyber security risks and vulnerabilities. To be responsible for the administration, configuration, and development of these technical areas both on-prem and cloud. Manage the effectiveness of operational cyber security and identify changes which will improve performance.
* To work with the ICT Infrastructure manager to develop the cyber security road map in line with the Digital and Data Strategy and implement the outcomes required, that drives changes throughout the business and its partners.
* Set best practice and policies within the cyber security provision across Digital and Data and the wider business, creating and maintaining standard operating procedures and technical system documentation as required.
* To offer 3rd line IT support to all levels and areas of the business, acting as one of a team of Principal Digital and Data Specialists for escalation on Digital and Data issues and Cyber Security incidents.
* Responsible for the delivery of multiple significant, highly complex, support issues and projects, meeting deadlines in a demanding environment.
* Responsible for identifying, evaluating and implementing solutions based on business need, utilising best practice within the team, and following IT Industry standards.
* Responsible for working on own initiative, managing time and making relevant technical decisions in accordance with best practice and the Digital and Data strategy.
* Assist in the professional development of junior members of the department acting as a mentor when required.
* To take part and lead in knowledge transfer where required to members of the relevant D&D teams to ensure greater skills resiliency and redundancy.
* Instil a culture of automation across all Cloud and On-Premises workloads, making recommendation of improvements to existing processes and products and working with business teams to achieve this.
* Identify and manage risks, issues, dependencies, and opportunities within the operational cyber security provision of the organisation. Ensure that the cyber security practice supports the organisation rather than restricts it.
* Responsibility for the backup, restore and performance of cloud and on-prem cyber security systems, ensuring robust and fault tolerant security systems are accessible and data is recoverable in a disaster recovery scenario.
* Work closely with the D&D department and wider business, including partners, to ensure the capture of all relevant data in a scalable environment and further develop the operational cyber security architecture to support at an enterprise level.
* Work closely with the Security & Information risk advisor and the Data Protection Officer to ensure required standards are met by implementing solutions and tools that monitor and enforce policies.
* Work with external suppliers and consultants in implementing solutions utilising best practice and compliance with WMCA standards and policies.
* Work with new and emerging cloud technologies to provide a modern, scalable architecture.
* Participate in the Out of Hours 24 / 7 support rota for business-critical systems where required.

**People Management**

* The role holder will be responsible for overseeing contractors and / or 3rd party suppliers to meet predefined outcomes.

**Decision Making Authority**

* The role holder will have delegated decision-making authority across areas of responsibility as set out by the Head of IT Delivery

**Person Specification**

|  |  |
| --- | --- |
| ***Please specify (X) whether the experience required is Essential (E) or Desirable (D)*** | **Assessment Method** |
| **Experience** | **E** | **D** | **App\*** | **Int\*\*** | **Other\*\*\*** |
| Experience in conducting risk assessments, vulnerability assessments, security compliance checks and external security audits. | x |  | x | x |  |
| Experience in regularly conducting penetration testing and remediation in accordance with an appropriate methodology. | x |  | x | x |  |
| Experience and understanding of business continuity and disaster recovery planning. Working with the wider D&D teams, responding to security threats, technical remediation, and root cause analysis. | x |  | x | x |  |
| Experience of deploying hybrid cloud operational cyber security systems including but not limited to Microsoft 365 security compliance features, identity and access management, threat protection, patch management and email / web security filtering. | x |  | x | x |  |
| Experience with Azure virtual instances, M365 environments and modern hybrid cloud architecture. |  | x |  |  |  |
| Experience of undertaking appropriate impact assessment of new and evolving security threats. | x |  | x | x |  |
| Experience with integrations and migration paths from on-prem solutions to cloud solutions. | x |  | x | x |  |
| Experience of analyzing highly complex technical issues and proposed solutions. | x |  | x | x |  |
| Experience in the design of operational cyber security systems and governance. | x |  | x | x |  |
| **Skills/Knowledge/Abilities** | **E** | **D** | **App\*** | **Int\*\*** | **Other\*\*\*** |
| In-depth knowledge of cyber security tools and best practices such as NCSC, OSNIT and IoCs. Familiar with security frameworks and regulations such as NIST, MITRE ATT&CK, GDPR and PCI DSS. | x |  |  |  |  |
| Strong understanding of security controls and procedures, including firewalls, IDS/IPS, DLP systems, SIEM, SOC, vulnerability management and threat protection. | x |  |  |  |  |
| Strong knowledge of security incident response plans and processes, proficient in leading, executing and coordinating security response plans and security investigations. | x |  |  |  |  |
| Demonstrated ability to manage multiple priorities and meet deadlines in a demanding environment. | x |  |  |  |  |
| Excellent communication and people skills, with the ability to effectively collaborate with stakeholders at all levels of the organization.  | x |  |  |  |  |
| Ability to tailor communication and information depending on the audience and being concise with the information requested / required. | x |  |  |  |  |
| Strong attention to detail and excellent customer service ethos. | x |  |  |  |  |
| Strong technical and governance documentation skills. | x |  |  |  |  |
| Ability to work autonomously and as a team player. | x |  |  |  |  |
| Evidence of outstanding working relationship with end users in exceeding their expectations. | x |  |  |  |  |
| Working knowledge of PaaS, SaaS and IaaS technologies. | x |  |  |  |  |
| Knowledge of scripting technologies, specifically for systems administration. |  | x |  |  |  |
| Virtual server environments. |  | x |  |  |  |
| An understanding of ITIL practices, current GDPR and information security principles. | x |  |  |  |  |
| **Qualifications/ Professional Memberships** | **E** | **D** | **App\*** | **Int\*\*** | **Other\*\*\*** |
| Qualified to degree level in a cyber security related discipline. | x |  |  |  |  |
| An IT cyber security technical qualification e.g. Certified information systems security professional (CISSP), Microsoft certified Azure security engineer or similar recognized professional qualification that demonstrates knowledge of essential skills. | x |  |  |  |  |
| ITIL Foundation Certificate is desirable. |  | x |  |  |  |

*\* Application \*\* Interview \*\*\* Details will be shared at interview stage*

**Core Expectations**

Our culture is underpinned by what we do and how we do it. Our behaviours outline the ways we need to work to deliver success, become truly inclusive, and make the organisation somewhere where everyone can give their best contribution.

|  |  |  |
| --- | --- | --- |
| **Value** | **Competency** | **Behaviour** |
| **Collaborative** | Team Focused | Works as part of team, managing and leading. |
| Service Driven | Customer, resident, and partner focused. |
| **Driven** | Empowered & Accountable | Takes ownership and leads when needed. |
| Performance Focused | Ambitious and going the extra mile. |
| **Inclusive** | ‘One Organisation’ Mindset | Believe in each other’s expertise. |
| Open & Honest | We do what we say we are going to do. |
| **Innovative** | Forward Thinking | Embrace change and open to new possibilities. |
| Problem Solving | Go for clear and simple whenever possible. |

**Health and Safety**

All employees have a duty to take reasonable care for the health and safety of themselves and of other persons who may be affected by their acts or omissions at work; and co-operate with their employer so far as is necessary to enable it to successfully discharge its own responsibilities in relation to health and safety.

**Equality and Diversity**

To promote and champion equality and diversity in all aspects of the role

**Learning and Development**

To participate in and take responsibility of any learning and development required to carry out this role effectively.

**Performance Management**

To actively engage in the performance management process and take responsibility for managing performance outcomes.

**GDPR (General Data Protection Regulation)**

To ensure the reasonable and proportionate protection, processing, sharing, and storing of WMCA information in accordance with the relevant legislation, corporate policies, and in the best interests of the data subjects (Data Protection/GDPR), the WMCA, our partners, and the West Midlands, in all aspects of the role.

**Other**

* There will be a requirement to ensure that support is provided between 08:00 – 17:00 Monday to Friday excluding bank holidays.
* There will be a requirement to work outside normal office hours to support WMCA’s Digital and Data systems
* There will be a requirement to work at any organisation sites as required and travel may be required on occasion
* There will be a requirement to participate in the D&D Out of Hours shift rota