**JOB DESCRIPTION**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **JOB DETAILS** | | | | |
| **Post title:** | **Networks and Cyber Manager** | | | |
| **Post grade:** | **H (with £12,000 market supplement)** | | | |
| **Directorate:** | **Transformation** | | | |
| **Section:** | **Digital Services** | | | |
| **Reporting to:** | **AD: IT, Cyber & Digital** | | | |
| **Line manager:** | **Yes** | | | |
| **Date updated:** | **August 2025** | | | |
|  | | | | |
| **MAIN PURPOSE OF JOB** | | | | |
| The Networks and Cyber Manager role is responsible for overseeing network and infrastructure configuration and security measures, managing cybersecurity protocols, and ensuring compliance with industry standards. The ideal candidate should possess proficiency in network and infrastructure management, experience with cybersecurity tools, and strong analytical skills. The role is responsible for a team of three Network and Cybersecurity Engineers. The role will ensure best practice is in place and that staff are trained to mitigate cyber risk. Additionally, the manager will handle various network infrastructure and cybersecurity projects, ensuring timely completion and maintaining budgetary constraints. Developing and implementing incident response plans, conducting regular security audits, and staying updated with the latest threats and vulnerabilities are also key responsibilities. | | | | |
|  | | | | |
| **SPECIFIC DUTIES** | | | | |
| The Networks and Cyber Manager is responsible for delivering robust, secure, and sustainable technology for the council. This involves creating security standards and policies to secure the council’s data and technology, making technology choices and trade-offs, and providing advice across various business areas. The manager must simplify complex information to create a blueprint that can be easily followed. Additionally, the role includes designing overall council-wide security solutions, policies, and designs, as well as reviewing services to analyse and assess their vulnerabilities. The manager will build and execute plans to mitigate these vulnerabilities and lead a program of penetration testing across the council to ensure systems are continuously improved to minimize security risks.  The manager is also tasked with identifying and mitigating technology-related risks by coordinating risk assessments and managing and monitoring the status of risks on an ongoing basis. Keeping up-to-date with emerging technology trends and developments is crucial, as the manager will seek to identify where technology might be deployed to deliver business improvements. Ensuring the design, maintenance, and documentation of group policy, active directory, DNS, and DHCP are well implemented and reviewed is another key responsibility.  The postholder will manage or undertake technology procurement for the council and ensure that network security policies, including firewall, proxy, endpoint protection, and virus checker, are well implemented and constantly reviewed. Following change management procedures correctly and ensuring the Council’s Backup and Disaster Recovery (DR) solution is well configured, maintained, and reviewed, including following the Disaster Recovery Plan if DR is invoked, are also essential duties. The manager will liaise with third-party suppliers and partners regarding support and ongoing relationships | | | | |
|  | | | | |
| **ORGANISATIONAL CHART** | | | | |
|  | | | | |
|  | | | | |
| **KEY WORKING RELATIONSHIPS** | | | | |
| The postholder will be responsible for three team members in the Networks and Cyber team. The postholder will work closely with the IT support manager to successfully manage the IT and technology offering across the organisation, supporting and training first line staff. | | | | |
|  | | | | |
| **RESOURCES** | | | | |
| The postholder will be responsible for the Cyber security budget within Digital Services and will be expected to maintain a high level of compliance with PSN code of connection, PCI DSS, DWPs memorandum of understanding and the cyber assessment framework. | | | | |
|  | | | | |
| **PHYSICAL DEMANDS** | | | | |
| The postholder will be subject to some physical demands, assisting team members with installing new hardware such as servers or switches. They may also be subject to occasional long hours during the event of an outage of cyber incident. | | | | |
|  | | | | |
| **MENTAL DEMANDS** | | | | |
| The postholder will have access across vast portions of the network and infrastructure, this may result in them being subject to sensitive or distressing information. There will often be conflicting demands across the team, the postholder will be expected to prioritise and lead the team through changing and competing priorities.  The postholder may have to perform occasional lone working. | | | | |
|  | | | | |
| **WORKING ENVIRONMENT** | | | | |
| The postholder will be expected to work from the Tewkesbury offices at least three days per week and may work the remainder from home if their home environment is in compliance with the remote working policy. | | | | |
|  | | | | |
| **ALL STAFF RESPONSIBILITIES** | | | | |
| To adhere to all Council Policies, in particular Equal Opportunities.  To undertake any other duties properly assigned from time to time by your line manager which are appropriate to the grade and character of the post.  To be committed to the principles of equality, diversity and the ability to treat everyone who you come in contact with dignity and respect.  Tewkesbury Borough Council is committed to the principles of safeguarding and promoting the welfare of all children, young people and vulnerable adults; therefore, all employees have a responsibility and duty of care to report safeguarding issues they become aware of or witness. | | | | |
|  | | | | |
| **HEALTH AND SAFETY** | | | | |
| Ensuring that services are delivered in compliance with existing and new Health and Safety legislation and the Council’s Health and Safety Policy and ensuring that duties are pursued in a safe manner with due regard to the Health and Safety of yourself and others.  To manage risk and to help formulate and comply with the Council’s Corporate Health, Safety and Welfare Plan, and to ensure that both systems and premises under your control are maintained in an acceptable standard to ensure the risk management and health and safety of staff and visitors. | | | | |
|  | | | | |
| **PERSON SPECIFICATION** | | | | |
| **QUALIFICATIONS** | | **ESSENTIAL** | **DESIRABLE** | **ASSESSMENT METHOD** |
| Vocational or professional qualifications in a relevant discipline | |  |  | Application |
| Educated to degree level or equivalent experience in IT | |  |  | Application |
| Relevant cybersecurity qualification (e.g. CISSP) | |  |  | Application |
| Evidence of continuous professional development (e.g. ITIL, CompTIA, MCSE) | |  |  | Application |
| **EXPERIENCE** | | **ESSENTIAL** | **DESIRABLE** | **ASSESSMENT METHOD** |
| Substantial ICT experience incl. VMWare, switching, firewalls, hardware/software/network design | |  |  | Application/Interview |
| Strategy and policy development/delivery | |  |  | Application/Interview |
| Balancing user, organisational and technical needs | |  |  | Interview |
| Running procurement projects | |  |  | Application/Interview |
| Team leadership or line management | |  |  | Application/Interview |
| Server installation and support in virtualised environments | |  |  | Application/Interview |
| Backup and disaster recovery solutions | |  |  | Application/Interview |
| Analysing and documenting user requirements | |  |  | Application |
| Public sector experience | |  |  | Application |
| **SKILLS** | | **ESSENTIAL** | **DESIRABLE** | **ASSESSMENT METHOD** |
| Excellent interpersonal skills | |  |  | Interview |
| Expert knowledge of security/system design, tools, platforms, best practices, trends and risks | |  |  | Interview |
| Deep knowledge of modern tech and security practices (services, infrastructure, hosting, platforms) | |  |  | Interview |
| Ability to present complex technical ideas simply | |  |  | Interview |
| Ability to identify and mitigate technology risks and vulnerabilities | |  |  | Interview |
| Comprehensive knowledge of VMWare, networking, Microsoft server | |  |  | Interview |
| Strong communication skills across all levels | |  |  | Interview |
| Project management and organisational skills | |  |  | Interview |
| Knowledge of managing/securing Linux environments | |  |  | Application/Interview |
| **BEHAVIOURS / ATTRIBUTES** | | **ESSENTIAL** | **DESIRABLE** | **ASSESSMENT METHOD** |
| Team player | |  |  | Interview |
| Innovative and research-driven | |  |  | Interview |
| Service delivery focused | |  |  | Interview |
| Works well under pressure | |  |  | Interview |
| Supports users with varying IT capabilities | |  |  | Interview |
| Committed to equality and diversity | |  |  | Application/Interview |