|  |  |
| --- | --- |
| **Job Description** | |
| **JOB TITLE** | **Cyber Security Analyst** |
| **JOB FAMILY** | **Technology** |
| **PHASE**  **PAY GRADE** | **Central**  **7** |
| **HOURS** | **Full time position (37 hours per week)** |
| **REPORTING TO** | **Head of IT Systems and Infrastructure** |
| **RESPONSIBLE FOR** | N/A |
| **Job Purpose** | |
| * + The Cyber Security Analyst supports the Trust’s Cyber Security Strategy and plays a vital role in protecting critical infrastructure, systems, services and data. This is a strategic and hands-on role covering technical security, governance, compliance, incident management, disaster recovery, training, and AI assurance. The postholder will work across teams to improve the Trust’s security posture, raise awareness, and help ensure the secure use of evolving technologies, including AI. | |
| **Duties and Responsibilities** | |
| **Cyber & Information Security Operations**   * Monitor and investigate security risks and alerts from all Trust systems, including Microsoft Entra, Aruba Central, Aruba Clearpass, firewalls, filtering, anti-virus and backup. * Perform regular vulnerability assessments and support remediation efforts. * Maintain oversight of privileged access, authentication, and audit logging across all Trust systems.   **Governance, Risk & Compliance**   * Maintain and update the cyber risk register, identifying and mitigating risks. * Contribute to the review and development of the Trust’s IT policies, with a focus on cyber security. * Participate in the Change Advisory Board (CAB) to assess, submit, and track security relevant changes. * To manage the Trust’s compliance against frameworks such as Cyber Essentials, ISO 27001, and DfE Digital Standards for Schools. * Utilise third-party tools and frameworks where possible to improve the Trust’s risk management and security posture. (e.g. CIS Benchmarks) * To create and present cyber security papers for the Trust’s Committees (Audit & Risk, Operations Committee) * Gain buy-in from senior leaders and key stakeholders for security changes that may have an impact on staff and student user experiences.   **Change Management & Rollout**   * Support the deployment of infrastructure or security changes, including testing, documentation, communication and handover. * Ensure that security controls are embedded during rollout of new platforms, services, and updates. * Regularly undertake reviews of all Trust systems to identify configuration drift and log incidents to ensure that un-intended changes are rolled back or fixed forward.   **Data Protection & DPIAs**   * Contribute to the review and creation of Data Protection Impact Assessments (DPIAs). * Advise on the appropriate technical and organisational controls for all services handling personal data. * Collaborate with the Governance & Compliance team and service managers to align security controls with data protection and privacy requirements.   **Incident Response & Cyber Exercises**   * Act as the lead responder to cyber incidents, coordinating technical investigation containment and remediation. * Maintain incident response forms, documenting the root cause, actions taken and lessons learnt. * Coordinate cyber incident simulations, such as NCSC’s Exercise in a Box, focusing on developing end user training/communication post simulations. * To act as the ‘lead communicator’ from an IT perspective across the organisation in response to cyber incidents, or configuration changes that will improve the Trust’s cyber security posture.   **Backup & Disaster Recovery**   * Regularly assess the Trust’s backup strategy, including retention, encryption, off-site replication, and testing. * Conduct scheduled disaster recovery testing to validate the integrity of data and accuracy of the disaster recovery processes. * Contribute to the development and improvement of Business Continuity Plans and Disaster Recovery documentation.   **Security Awareness & Training**   * Develop and deliver cyber security training and guidance for staff, governors and pupils (where relevant), tailored to their roles, risks and access levels. * Support communication campaigns across the organisation to promote security awareness and best practices. * Develop and undertake phishing simulations and integrate findings into user training/communication post simulations.   **AI Governance & Emerging Technologies**   * Contribute to the secure and ethical development and adoption of AI technologies across the Trust. * Support the creation of risk assessments, policies, and security best practises for AI tools & services. * Collaborate with data and digital stakeholders to ensure responsible and compliant use of AI across all functions.   **Strategic Contribution**   * To develop the Trust’s Cyber Security Strategy, feeding into roadmaps, audits, and the wider technical development of Trust systems, following industry best practice as much as possible. * Stay current with evolving cyber threats, technologies, and compliance expectations. * Identify, recommend and implement security enhancements across all Trust systems and services (on-prem and cloud hosted environments/services). | |
| **Generic Duties relevant to all members of Staff** | |
| Working with colleagues and other relevant professionals   * Create, maintain and develop positive and effective working relationships both with and between pupils, colleagues, parents and carers, governors, Trust members and other stakeholders * Communicate effectively with other staff members, customer and service users * Collaborate and work with colleagues and other relevant professionals within and beyond the Trust * Develop effective professional relationships with colleagues   Professional development   * Help keep their own knowledge and understanding relevant and up-to-date by reflecting on their own practice, liaising with their line manager and identifying relevant professional development to improve personal effectiveness * Take opportunities to build the appropriate skills, qualifications, and/or experience needed for the role, with support from the Trust * Take part in the Trusts appraisal and performance management procedures   Personal and professional conduct   * Uphold public trust in the education profession and maintain high standards of ethics and behaviour, within and outside school * Have proper and professional regard for the ethos, policies and practices of the Trust, and maintain high standards of attendance and punctuality * Demonstrate positive attitudes, values and behaviours to develop and sustain effective relationships with the Trust community * Respect individual differences and cultural diversity   Equal Opportunities   * + To actively promote the Trust’s Equal Opportunities Policy and observe the standard of conduct which prevents discrimination taking place, maintaining awareness of and commitment to Equal Opportunity Policies in relation to both employment and service delivery.   The Trust   * The ethos of our Trust is “Transforming Life Chances”. All staff are expected to be committed to this aim in everything they do. * It is expected that all staff work collaboratively as members of the Trust to share good practice, resources and ideas and realise the Trust’s visions and aims. All staff should act with professional integrity at all times, following the “Code of Conduct”. * You will be based at TSAT Hub. However, you may be asked to work at any of the other Hubs within the Trust and you should expect to travel between sites as required.   Teaching and Learning   * This is our core business and therefore it is an absolute priority. You are expected to support all teaching staff, irrespective of seniority, to ensure they concentrate on the core business. This may mean undertaking tasks outside of your area of responsibility where required.   Customer Service   * At TSAT customer service is paramount to our way of work; All staff will be required to mirror our philosophy and take pride in offering a fantastic customer experience to all stakeholders modelled on our four Customer First Values - Trusted, Solution Focused, Approachable & Timely   ICT   * It is expected that all teaching and support staff follow the ICT Vision of the Trust. * All staff will be expected to utilise ICT and to improve communication and reduce paper use. Security procedures must be followed when using ICT systems. * All staff are expected to follow the procedures as laid out in the Trust’s Acceptable Use Policy. Staff are also expected to ensure that they follow Trust policies with regard to professional conduct when using ICT systems or Trust ICT equipment.   Health and Safety   * Employees are required to work in compliance with the Academy’s Health & Safety Policies and under the Health and Safety At Work Act 1974 (as amended), ensuring the safety of all parties they come into contact with, such as members of the public, in premises or sites controlled by the Trust. * In order to ensure compliance, procedures should be observed at all times under the provision of safe systems of work through safe and health environments, including information, training and supervision necessary to accomplish those goals.   Safeguarding   * The Thinking Schools Academy Trust is committed to safeguarding and promoting the welfare of children and young people and all staff must ensure that the highest priority is given to following the guidance and regulations to safeguard children and young people. All staff are to have due regard for safeguarding and promoting the welfare of children and young people and to follow the child protection procedures adopted by the Thinking Schools Academy Trust. Any safeguarding or child protection issues **must** be acted upon immediately by informing the Designated Safeguarding Lead.   Data Protection   * The Thinking Schools Academy Trust takes the responsibility of protecting and securing the data of Pupils, Staff, Parents and all associated individuals very seriously. The Trust requires all staff to complete data protection training and to adhere to its Data protection policies and procedures. All staff must ensure that if they suspect a data breach they must inform the Trust Data Protection officer immediately. | |

This job description forms part of the contract of employment of the person appointed to the post.  The duties, responsibilities and accountabilities highlighted in this job description are indicative and may vary over time at the discretion of the Trust.  This job description will be reviewed annually and is an integral part of the Appraisal and line management process.

The duties and responsibilities in this job description are not restrictive and the post-holder may be required to undertake any other duties that may be required from time to time.  Any such duties should not however substantially change the general character of the post.

I understand and agree to the job description of Infrastructure Security Analyst.

Name:                                                               Signed:                                                   Date:

|  |  |
| --- | --- |
| **Personal Specification** | |
|  | E = Essential / D = Desirable |
| **Experience Knowledge** | |
| |  |  | | --- | --- | | Demonstrable experience (3–5 years) working in an IT security, infrastructure, or systems administration role, with direct responsibility for cyber security. | E | | Knowledge of cyber threats, attack vectors, and mitigation techniques relevant to education or public sector environments. | E | | Experience of implementing and managing security tools and technologies (e.g. endpoint protection, SIEM, firewalls, vulnerability scanners, EDR/XDR) | E | | Familiarity with Microsoft 365 security, Azure/Entra ID, and Intune compliance policies | E | | Understanding of data protection legislation (UK GDPR, Data Protection Act 2018) and their impact on IT security in schools and public sector bodies | E | | Knowledge of cyber security frameworks and standards such as Cyber Essentials Plus, CIS Benchmarks, NCSC guidance, and ISO 27001 | E | | Practical experience of investigating and responding to security incidents | E | | Awareness of safeguarding and child protection considerations in relation to ICT systems in education | E | | Experience working with third-party providers and managed services within education or the public sector | D | | Experience of/familiarity with operating system scripting (i.e. PowerShell, VBS, BAT, BASH, Python). | E | | Experience of Service Request Management systems (i.e. TopDesk, SysAid). | E | | |
| **Skills/Abilities** | |
| |  |  | | --- | --- | | Ability to assess and interpret security logs, alerts, and reports to identify and mitigate risks | E | | Strong analytical and problem-solving skills with a proactive approach to cyber threat detection and prevention | E | | Capable of translating complex technical issues into clear advice and guidance for non-technical staff and leadership teams | E | | Effective organisational skills with the ability to prioritise competing demands across multiple schools/sites | E | | Ability to conduct risk assessments and produce actionable recommendations | E | | Strong interpersonal skills with the ability to influence and build relationships with a range of stakeholders including school leaders, IT teams, and external partners | E | | Ability to work independently as well as collaboratively in a team across a distributed environment | E | | Commitment to continuous professional development and keeping up to date with emerging threats and technologies | E | | Ability to use knowledge of relevant legislation including Computer Misuse, Acceptable Use Policies, Data Protection and Child Protection to monitor the use of ICT systems, and develop or improve existing processes. | E | | Ability to create both technical and non-technical documentation using a range of software and tools, including, word-processing, spreadsheets, and presentation applications. | E | | |
| **Qualifications and Training** | |
| |  |  | | --- | --- | | Degree in Computer Science, Information Security, or related discipline; or equivalent professional experience | E | | Industry-recognised cyber security certification(s) such as CompTIA Security+, Microsoft SC-200/SC-900, or equivalent as a minimum | D | | Advanced certifications such as CISSP, CISM, CCSP, or equivalent (not essential but advantageous) | D | | Evidence of ongoing professional development (e.g., NCSC training, vendor certifications, or relevant CPD) | E | | ITIL Foundation or equivalent service management training | D | | Current or willingness to achieve Cyber Essentials Plus assessor training | D | |  |  | | |
| **Attributes** | |
| |  |  | | --- | --- | | Ability to work under pressure to meet deadlines. | E | | Excellent organisational and time management skills with the ability to use initiative and prioritise a wide-ranging workload with competing demands. | E | | Excellent interpersonal skills – establishing relationships and maintaining contacts with people from a variety of backgrounds. | E | | Ability to communicate effectively with patience and politeness with all contacts, from students to senior management, whether verbally or in writing. | E | | Ability to work with and assist, both remotely, and if required in person (through travelling), all academies and partners within The Thinking Schools Academy Trust. | E | | Self-motivated, proactive team player. | E | | Full UK Driving License, with access to own transportation. | E | | High level of accuracy and attention to detail. | E | | A commitment to customer service. | E | | A commitment to equality and diversity. | E | | |