Job Description: Cyber Security Analyst

Reports to: IT Infrastructure Manager
Location: Within London, Portsmouth, Hastings, and Birmingham
Contract: Permanent
Pattern: Full Time
Salary: £35,000
Start Date: ASAP

About the role:

We are seeking an experienced Cyber Security Analyst to join our IT Infrastructure team. The Cyber Security Analyst will be responsible for ensuring the security of our information systems, networks, and data, as well as identifying and responding to potential security threats. The Cyber Security Analyst will report directly to the IT Infrastructure Manager and work closely with the IT Teams and Ark's service partners to maintain the integrity and confidentiality of our digital assets.

This is an exciting opportunity to make a lasting and positive impact on Ark's support of IT across its network. The Cyber Security Analyst will be working with an innovative and forward-thinking Head of IT and Systems and a tightly integrated IT and Systems team, with an opportunity to contribute to the delivery of a new Ark IT Strategy.

Key Responsibilities:

- Monitor updates for all major systems used within the Ark estate for security vulnerabilities
- Ensure that all systems and devices are up to date
- Collaborate with other teams, to ensure security is integrated into all aspects of the organisation's systems and processes
- Ensure update compatibility with current hardware
- Conduct regular security awareness training to educate both technical and nontechnical staff on best practices for information security
- Ensure that any major change or updates to systems are submitted to CAB prior to implementation
- Liaise with the IT Infrastructure Teams, Service Delivery Managers, Team Leaders, and Technicians to resolve security concerns
- Monitor tools such as Sophos, Malwarebytes and Risky Users and any other cyber related dashboard for issues and escalate accordingly
- Ensure that all cyber security related tasks are completed to a high standard
- Assess the output of vulnerability scans and address all medium, high and critical alerts with the help of the Infrastructure Team and service partners
- Develop and implement security policies, procedures, and guidelines to ensure the protection of our information systems, networks, and data
- Respond to and investigate security incidents and help to develop and implement remediation plans

Person Specification: Cyber Security Analyst

Knowledge & Skills

- Broad experience, ideally gained within the education sector, of technical delivery, including; infrastructure, networking, perimeter security, monitoring/operating/database systems and threat detection
- Evidence of an understanding of current technologies within the education sector, with a keen interest in further developing their skills in accordance with evolving trends
- Exceptional judgement and decision-making skills when resolving challenging issues; knowing when to appropriately sign post and escalate
- Strong research and organisational skills, to produce professional written reports and/or material for presentations
- Maintain essential IT operations, including operating systems, security tools, applications, servers, email systems, laptops, desktops, software, and hardware
- Excellent working knowledge of:
    - Microsoft Active Directory environment
    - Microsoft 365 and SharePoint
    - Teams unified communications
    - Azure Identity and access management
    - Cisco Meraki, wireless, switching, CCTV and EMM
    - Windows 10 and macOS
    - Microsoft Endpoint Manager and MDM solutions
    - Print Solutions such as PaperCut
    - Windows Server environment
    - Virtualisation technologies such as Hyper-V
    - School MIS systems such as Bromcom and Scholar pack
    - Windows Group Policy
    - Google Gsuite and other cloud platforms
    - Azure Active Directory and Azure IaaS and PaaS
    - EDR Solutions
    - SOC tools and solutions

Personal Qualities

- The drive and ability to motivate, guide and mentor team members in technical delivery
- Own and lead on technical projects, solutions, and key responsibilities within the larger organisational initiative

Other

- Right to work in the UK
- Commitment to equality of opportunity and the safeguarding and welfare of all students
- Willingness to undertake training
- This post is subject to an enhanced DBS check

Ark is committed to safeguarding and promoting the welfare of children and young people in its academies. In order to meet this responsibility, its academies follow a rigorous selection process to discourage and screen out unsuitable applicants.

Ark requires all employees to undertake an enhanced DBS check. You are required, before appointment, to disclose any unspent conviction, cautions, reprimands or warnings under the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975. Non-disclosure may lead to termination of employment. However, disclosure of a criminal background will not necessarily debar you from employment - this will depend upon the nature of the offence(s) and when they occurred. To read more about Ark's safer recruitment process, please click this link.

We aim to build a diverse and inclusive organisation where everyone – staff and students – can do their best work and achieve their full potential. We want to reflect and represent diverse perspectives across our organisation because we know that doing so will make us stronger and more effective. To know more about Ark's diversity and inclusion commitments, please click on this [link.](link)