Staffordshire University Services Limited

Job Description

Job Title	Cybersecurity Analyst
School/Service/Institute	Digital Services
Normal Workbase	Stoke
Tenure	Permanent
Grade/Salary	Grade 7
FTE/Hours	1.0 fte

Job Purpose
• Responsible for the implementation and operation of information security controls to maintain the confidentiality, integrity, availability, accountability, and relevant compliance of information systems with legislation, regulation and relevant standards. • Responsible for ensuring appropriate implementation of information assurance policies so that stakeholder confidence that risk to the integrity of information, wherever and however it is held, is appropriately maintained in a cost-effective manner. • Conducts medium to complex cybersecurity investigations preparing formal forensic reports covering the collection, processing, preserving, analysing and presentation of computer related evidence in support of cybersecurity vulnerability mitigation and/or criminal, fraud, counter intelligence, or law enforcement investigations.

Relationships	
Reporting to:	Cybersecurity Manager
Responsible for:	No direct reports

Main Activities
• Conducts cybersecurity control reviews across a full range of control types and techniques, for business applications and computer installations. Seeks guidance from more experienced or specialised practitioners as required. Recommends appropriate action to management. • Identifies threats to the confidentiality, integrity, availability, accountability and relevant compliance of information systems. Conducts risk and vulnerability assessments of business applications and computer installations in the light of these threats and recommends appropriate action to management.

- Conducts investigation, analysis and review following breaches of cybersecurity controls, and manages cybersecurity incidents. Prepares recommendations for appropriate control improvements, involving other professionals as required.

- Provides authoritative advice and guidance on the application and operation of all types of cybersecurity controls, including legislative or regulatory requirements such as data protection and software copyright law. Contributes to development of standards and guidelines.

- Delivers and contributes to the design and development of cybersecurity education, training and awareness to management, staff and students including incident simulation and desktop exercises.

- Designs the security components of systems architectures.

- Interprets security and assurance policies and contributes to development of standards and guidelines that comply with these, to enable effective assessment of risks to information availability, integrity, authentication, and confidentiality.

- Carries out risk assessment of complex information systems and infrastructure components. Contributes to audits of information systems.

- Reviews compliance to information security policies and standards, configuration assessment, adherence to legal and regulatory requirements, and recommends appropriate action.

- Advises information and network users on Information assurance architecture and strategies to manage identified risk and promotes awareness of policies and procedures. Acts to ensure that they are aware of obligations such as protecting the secrecy of passwords and accounts access details.

- Assesses the effectiveness of firewalls, Gateways, IDS (Intruder Detection Systems) and IPS (Intruder Prevention Systems) to improve network/system resilience. Seeks to assure integrity of system interconnectivity at all layers of the OSI model.

- Monitors and tests network usage, for compliance with legal and policy requirements, to detect (for example) transmission of any offensive or indecent material and reports such incidents immediately to the appropriate authority.

- Supports initiatives addressing assurance of information in all formats, for example audits of physical information holdings.

- Leads automated and manual vulnerability assessments. Assesses effectiveness of cybersecurity controls for infrastructure and application components and recommends remedial action.

- Reviews compliance with information security policies and standards including technical assessments of DPIA and Data Sharing agreements. Assesses configurations and security procedures for adherence to legal and regulatory requirements.

- Lead social engineering activities such as phishing, pretext calling and in-person pretexting.
- Management and maintenance of Digital Systems relating to cybersecurity e.g SIEM (Security Incident Event Management), Vulnerability Management, and logging / reporting tools
- Provision of second line service desk for incidents and problems relating to cybersecurity.
- Support the cybersecurity manager in obtaining and maintaining relevant security certifications such as ISO27001 and Cyber Essentials Plus
- To undertake appropriate professional development and mandatory training activities as identified or required (See Professional Development section).
- The role holder is required to minimise environmental impact in the performance of their role and to actively contribute to the delivery of the University's Environmental Sustainability Policy

Special Conditions

In the event of a security incident the postholder may be required to undertake emergency out of hours activities, up to 4 hours / month on Saturday or Sunday, and up to 4 hours / month (Monday to Friday). The postholder will be entitled to time-off-in-lieu, to be recorded on a flexi-sheet and agreed in advance with their manager. As much notification as possible will be provided.

If, in exceptional circumstances, additional hours of evening/weekend work are required in any month, time-off-in-lieu or overtime would apply in accordance with the University Remuneration Policy.

Professional Development

The University will support and encourage the postholder to engage in continuous professional development activities through the YOURCareer@Staffs framework. This framework supports postholders to identify appropriate development opportunities. Continuing Professional Development (CPD) activity will be recognised by a bi-annual Performance and Development Review (PDR) discussion.

Variation to Job Description

The University reserves the right to vary the duties and responsibilities of its employees within the general conditions of the Scheme of pay and conditions and employment related matters. Thus, it must be appreciated that the duties and responsibilities outlined above may be altered as the changing needs of the service may require.

Conditions of Service

The postholder will be employed by Staffordshire University Services Limited.

Staffordshire University Services Limited is a wholly owned subsidiary company of Staffordshire University which recruits and provides both academic and professional support staff to the University. You will be subject to Staffordshire University's policies and procedures and will be eligible to participate in the Staffordshire University Pension Scheme.

Application Procedure

We encourage applicants to apply on-line at our website http://jobs.staffs.ac.uk as the system is user friendly and simple to complete.

We ask that all applicants ensure that they have provided comprehensive information under each criterion in the Supporting Statements section of the application form and, if necessary, add any relevant additional information in the Additional Information Section.

The University will use anonymous application forms for this role; however, we recognise that applicants may want to include additional information. If you choose to upload any supporting documents that contain identifiable data, your application will no longer be considered anonymous.