Staffordshire University Services Limited

Job Description

Job Title	Cybersecurity Manager
School/Service/Institute	Digital Services
Normal Workbase	Stoke
Tenure	Permanent
Grade/Salary	Grade 9
FTE/Hours	1.0 fte

Job Purpose
• Responsible for the development and implementation of Digital Security policy in order to assure the confidentiality, integrity, availability, accountability and relevant compliance of University information systems with the relevant legislation, regulation and standards. The role provides expert advice on, the selection, design, justification, implementation and operation of information security controls and management strategies, leading rapid response should a security breech occur. The Cybersecurity Manager is also responsible for the leadership and oversight of information assurance, designing and implementing high level strategy and policy, to ensure stakeholder confidence that risk to the integrity of information on premise or in the Cloud; in storage or in transit is managed pragmatically, appropriately and in a cost effective manner.

Relationships	
Reporting to:	Head of Cybersecurity, Risk and Compliance
Responsible for:	Cybersecurity Analyst, Cybersecurity Apprentice

Main Activities
• Develops digital information security policy, standards and guidelines appropriate to business, technology and legal requirements and in accordance with best professional and industry practice. • Prepares and maintains a business strategy and plan for information security work which addresses the evolving business risk and information control requirements, and is consistent with relevant digital and business plans, budgets, strategies, etc. • Manages assessment of threats to confidentiality, integrity, availability, accountability, and relevant compliance. Takes ownership of security control reviews, business risk assessments, and reviews that follow significant breaches of security controls

- Operates as a focus for digital security expertise for the organisation, providing authoritative advice and guidance on the application and operation of all types of security control, including legislative or regulatory requirements such as data protection and software copyright law.
- Manages the work of all other digital security specialist staff, including project and task definition and prioritisation, quality management and budgetary control, and management tasks such as recruitment and training when required
- Manages the operation of appropriate security controls as a production service to business system users
- Delivers the security components of Enterprise architectures
- Protects and defends information and information systems by defining digital policies to ensure their availability, integrity, authentication, confidentiality, and non-repudiation. Ensures that these policies permit individuals to access only information and network facilities for which they are authorized
- Assesses legal and best practice issues, and promotes awareness of national and international laws, including those relating to confidentiality, privacy, and copyright.
- Develops strategies for information assurance, as part of corporate digital governance, including guidelines for information and network users.
- Ensures architectural principles are applied during design to reduce risk, and advances assurance standards through ensuring rigorous security testing.
- Determines appropriate and practical performance measures, to ensure that information assurance priorities set by the business can be effectively monitored.
- In the context of Business Continuity, assesses protection, detection, and reaction capabilities, to determine whether they are sufficient to support restoration of information systems in a secure manner.
- Contributes to the development, implementation and monitoring of organisational policies and processes intended to maintain the availability, integrity and confidentiality of the organisations information assets
- Advises at executive level on risk management policies, and assists with the creation and publication of strategies for managing risk to the continuing effective operation of the business.
- Identifies and categorises strategic and operational risks. Breaks down risks by sub-categories, such as compliance, architecture, environment, financial, etc.
- Advises on the evaluation of identified risks (including probability/frequency of occurrence, impact, and severity).
- Advises on appropriate action, including contingency planning, and countermeasures
- Motivates, leads and manage all direct line reports and other staff where required allocating responsibilities, work planning and managing performance. Provides general guidance, coaching and support, developing their skills, knowledge and understanding. Carries out regular appraisals, setting objectives, giving feedback and ensuring that targets met.
- Manages obtaining and maintaining relevant security certifications such as

ISO27001 and Cyber Essentials Plus

- 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.
- Management and maintenance of Digital Systems relating to cybersecurity e.g SIEM (Security Incident Event Management), Vulnerability Management, and logging / reporting tools
- 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.