Job Description

General Details

Job title:	Security Analyst (DS18-01)
School/Service:	Digital Services
Normal Workbase:	Stoke Campus
Tenure:	Permanent
Hours/FTE:	Full time working 37 hours per week
Grade/Salary:	Grade 6
Date Prepared:	May 2019

Job Purpose

Responsible for the operation of information security controls to maintain the confidentiality, integrity, availability, accountability and relevant compliance of information systems with legislation, regulation and relevant standards.

Monitors effectiveness of information assurance policies to evidence that they are 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:	Security Manager
Responsible for:	N/A

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 advice and guidance on the application and operation of all types of cybersecurity controls.

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.

- 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, and recommends appropriate action

- Advises information and network users on Information assurance 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

- Undertakes 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. Assesses configurations and security procedures for adherence to legal and regulatory requirements

- Undertakes social engineering activities such as phishing, pretext calling and in-person pretexting

Special Conditions

To be committed to working with the University to further improve the carbon footprint/environmental issues.

Variation to Job Description

The employer 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

If you are successful in being appointed to a professional support role at Grades 1-6, you will be employed by Staffordshire University Services Limited (SUS Ltd).

Staffordshire University Services Limited (SUS Ltd) is a wholly owned subsidiary company of Staffordshire University which provides professional support staff to undertake various roles and responsibilities associated with grades 1 to 6 on the Staffordshire University pay scale. You'll work alongside, and under the direction of colleagues, within the University's Schools and Services in the delivery of our University Plan and supporting KPIs. You will be subject to Staffordshire University's policies and procedures and will be eligible to participate in the Staffordshire University Services Limited (SUS Ltd) Pension Scheme

Informal Discussion

Should you wish to discuss this vacancy informally before making an application please contact:

Mark Hewitt, Cybersecurity Manager - Email m.a.hewitt@staffs.ac.uk or telephone 01785 353369

Application Procedure

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

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