Job Description

General Details	
Job title:	Security Analyst (DS17/18RA)
Faculty/School/Service:	Digital Services
Normal Workbase:	Stoke-on-Trent Campus
Tenure:	Permanent
Hours/FTE:	37 hours per week
Grade/Salary:	6
Date Prepared:	17/12/17

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 security investigations preparing formal forensic reports covering the collection, processing, preserving, analysing and presentation of computer related evidence in support of security vulnerability mitigation and/or criminal, fraud, counter intelligence or law enforcement investigations.

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

Main Activities
Conducts security 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 security controls, and manages security 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 security controls. Contributes to development of standards and guidelines.
Delivers and contributes to the design and development of specialist digital security education and training to digital and system user management and staff.

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 security 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

The role holder will be required to travel between sites from time to time in a cost effective manner, which may be through the use of a car.

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

Variation to Job Description

Staffordshire 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 post is subject to such terms and conditions of employment as negotiated between the Board of Governors of the University and the recognised trade unions, and/or the employees of the University. In negotiating such terms and conditions the Board of Governors will consider any appropriate advice received from the Universities and Colleges Employers Association (UCEA).

Informal Discussion

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

Mark Hewitt (Security Manager) E: m.a.hewitt@staffs.ac.uk T: 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.

Person Specification

Job Title: **Security Analyst (DS17/18RA)**
School/Service: **Digital Services**

The qualifications, experience, knowledge skills and personal qualities outlined below provide a summary of what is required to carry out this job effectively. They also form the selection criteria on which a decision to appoint will be made. Please ensure that you provide evidence of how you meet the criteria in your application.

No	Selection Criteria Description	Essential [E] or Desirable [D]	Assessed by *
1	**Security Awareness** A broad understanding of the current security threat landscape, existing and emerging technologies.	E	A/I
2	**Security Operation.** Understanding of requirements for maintaining security certifications such as ISO27001, Cyber Essentials or PCI. Experience in gathering operational evidence on the performance of cyber security within one or more of the following areas: using vulnerability assessment tools, assessing the effectiveness of firewalls, undertaking of penetration testing, using log analysis tools, monitoring use of privileges accounts or using SIEM tools.	E	A/I
3	**Analytical Thinking:** Understanding a problem or situation by breaking it down systematically into its component parts and identifying the relationships between these parts, selecting the appropriate method/tool to resolve the problem and reflecting critically on the result.	E	I
4	**Customer Focus.** Self-motivated, well organised and positive approach to work with the ability to manage and prioritise a complex workload and experience of dealing with challenging and demanding customers; whilst understanding the needs of the internal or external customer needs/requirements and regularly checking with the customer when taking actions or making decisions.	E	I
5	**Interpersonal, written and verbal communication skills:** Effective negotiation and influencing skills with demonstrable strong facilitation skills, excellent interpersonal, written and verbal communication skills with the ability to translate often complex information into easy to understand messages for a range of audiences.	E	I
6	**Team Work:** Effective and committed team player that is able to work successfully with others and to build positive working relationships.	E	I
7	**Security Response.** Experience in investigation, analysis and review following breaches of security controls. Managing security incidents using a methodology such as ITIL.	D	A/I
8	**Infrastructure Architecture.** An understanding the principles of physical, virtual and cloud architectures (IaaS, SaaS, PaaS) for systems and networks.	D	A/I

9	**Networking and Communications.** An understanding of networking and communications related concepts such as TCP/IP networking, DNS, DHCP, load balancing, firewalls, application firewalls, IPS/IDS.	D	A/I
10	**Access Control Systems.** Knowledge of authentication, monitoring and logging systems. Such as Active Directory, Azure Active Directory, Network Access Control, Multi-factor authentication systems, or SIEM tools.	D	A/I
11	**Risk Management**. An understanding of the methods and techniques for the assessment and management of business risk. Identifying threats to the confidentiality, integrity, availability, accountability and relevant compliance of information systems.	D	I
12	**CISSP –** Certified Information Systems Security Professional **BCS** - Data Protection (Practitioner) **BCS** - Certificate in Information Security Management Principles (Foundation) **CESG** - Certified Professional **BCS** - Chartered IT Professional (CITP) **Or equivalent qualification or experience**	D	A

***Key** **[A] Application form** **[I] Interview**	**To be assessed against the information provided in the relevant steps of the application form and the evidence required under Section 4, ‘Supporting Statements’** **To be assessed during the interview process including selection tests or presentation, as appropriate**