Job Description

Staffordshire University Services Limited

Job Title	Digital and Technology Solutions Professional Degree Apprentice (Cyber Security)
School/Service/Institute	Digital and Technical Services
Normal Workbase	Stoke
Tenure	Full Time Fixed Term Contract - 40 Months
Grade/Salary	4
FTE/Hours	1.0 FTE (with release for linked Academic Lectures & Learning Blocks)

Job Purpose

Staffordshire University has the ambition of becoming the leading digital university across the UK, transforming the student experience, and improving student success in an increasingly digitally led world.

The Digital and Technical Services is a professional service responsible for the University's overall use of digital and other teaching and learning technology to achieve the University strategy.

Working within the Cyber Security Team and Reporting to the Cyber Security Manager, the role of the Digital and Technology Solutions Professional Degree Apprentice (Cyber Security) will perform the following:

- Security event monitoring and management
- Initiate incident response
- Review and act on threat intelligence
- Undertake vulnerability management and liaise with Digital Services teams to remediate.
- Undertake security reviews and security control verification.
- Raise user awareness in all matters of Cyber Security

Relationships	
Reporting to:	Cyber Security Manager
Responsible for:	N/A
Key working relationships:	Cyber Security Team, Digital Services Team,

Main Activities
• Undertakes automated and manual vulnerability assessments. Assesses effectiveness of cybersecurity controls for infrastructure and application components and recommends remedial action. • Review security alerts & logs to detect potential cybersecurity incidents initiating the appropriate response. • 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. • Provides advice and guidance on the application and operation of all types of cybersecurity controls. • 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. • Contributes to the design and development of cybersecurity education, training and awareness to management, staff and students. • Supports initiatives addressing assurance of information in all formats, for example audits of physical information holdings. • Undertakes social engineering activities such as phishing, pretext calling and in-person pretexting.

Core Knowledge (To be acquired throughout Apprenticeship)
• How business exploits technology solutions for competitive advantage. • The value of technology investments and how to formulate a business case for a new technology solution, including estimation of both costs and benefits. • Contemporary techniques for design, developing, testing, correcting, deploying and documenting software systems from specifications, using agreed standards and tools. • How teams work effectively to produce technology solutions. • The role of data management systems in managing organisational data and information. • Common vulnerabilities in computer networks including unsecure coding and unprotected networks. • The various roles, functions and activities related to technology solutions within an organisation. • How strategic decisions are made concerning acquiring technology solutions resources and capabilities including the ability to evaluate the different sourcing options. • How to deliver a technology solutions project accurately consistent with business needs • The issues of quality, cost and time for projects, including contractual obligations and resource constraints

Specialist Technical Knowledge Objectives (To be achieved by end of the Apprenticeship Programme)
• The principles of threat intelligence, modelling and assessment. The range of modern attack techniques and how and where to research emerging attack techniques to inform the development of improved security controls, countermeasures and policies and standards; • How to use human factor analysis in the assessment of threats, including the motivations and methods adopted by a wide range of human threat actors; • How to select and apply tools and techniques to carry out a variety of security testing strategies including vulnerability scanning, penetration testing and ethical hacking, recognising that security testing itself cannot guarantee security and only reveal gaps in security provisioning; • The different approaches and design principles that are used to engineer secure systems, focusing on the importance of building in security, privacy and resilience in the initial design; • How to develop and implement security event response programmes, security event handling, and operational security activities; • The different types of cyber security controls that can be implemented, the main principles of secure configuration of security components and devices, including firewalls and protective monitoring tools and how to apply them.

Specialist Skills (To be acquired throughout Apprenticeship)
• Plan and carry out a variety of security testing strategies on IT infrastructures, middleware and applications, to identify new issues and recommend remediation and enhancements to security policies and information technology procedures; • Perform cyber threat intelligence analysis to research, analyse and evaluate technical threats by reviewing open source and other information from trusted sources for new vulnerabilities, malware, or other threats that have the potential to impact the organisation; • Identify, investigate and correlate actionable security events, including performing network traffic analysis using a range of techniques relevant to the security of communication networks to assess security risks and escalating where appropriate; • Conduct a vulnerability assessment, to identify and report on vulnerability issues and possible solutions arising, including recommending cost-effective mitigations comprising careful combinations of technical, procedural and administrative controls; • Select and apply cyber security forensic tools and techniques for attack reconstruction, including forensic analysis and volatile data collection and analysis; • Conduct analysis of attacker tools providing indicators for enterprise defensive measures including classifying and identifying attack patterns.

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 during the evening (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.