University of Sunderland

Role Profile

Part 1

lifechanging University of Sunderland

Cyber Security Officer

Job Title:	Cyber Security Officer
Reference No:	0558-21
Reports to:	Cyber Security Architect
Responsible For:	
Grade:	E
Working Hours:	37 hours for nominal purposes
Faculty/Service:	Technical Services
Location:	Sunderland Campus
Main Purpose of Role:	To contribute to the formulation, development and review of all University policies, processes and procedures which relate in any way to information and cyber security activities of the University. To be an active member of the University's Cyber Security Team that provides help and guidance to the entire University on cyber security. To ensure the IT operations and development activities of the University meet the required standards of the University's cyber strategy and any external stakeholders. To manage the formulation, development, delivery and continuous improvement of the Universities staff and student education and awareness programme.
Key Responsibilities and Accountabilities:	Analysis, Reporting and Documentation • To provide specialist advice and guidance to staff and students on cyber security. This involves risk management, assisting with the drafting of, and compliance with standards and providing authoritative advice to management and professional IT staff. • To assist with the development and maintenance of institutional policies, processes, procedures, guidelines, and standards which relate to the cyber security activities. • To support, and in the absence of, the Cyber Security Architect, reporting security issues to senior members. • Participate, where appropriate, in forensic evidence gathering, disciplinary measures and criminal investigations as part of the University's Technical Investigation Procedure. • Contribute to the production of IT systems architectures with associated security component specifications.

- Devise new or revised operational procedures relating to security controls of all IT environments, products or services ensuring that any system changes required to maintain security are implemented.

Security Operations

- Conduct security control reviews and business risk assessments across a full range of control types and techniques, for business applications, supporting infrastructure, managed services, and user interfaces.
- Identify and manage assessments of threats to the confidentiality, integrity, and availability of the IT estate.
- Formulate, develop, and implement IT security plans, taking into account current best practises, legislation and regulations to support the cyber security strategy to ensure an effective level of cyber hygiene is met.
- Influence the design, procurement and operational controls and the secure use of IT solutions.
- Provide technical management of the IT security operation, working to ensure agreed service levels are met and all relevant procedures are adhered to.
- Monitor the wider environment to gain knowledge and understanding of current emerging threats and report the risks posed to the University.
- Contribute to the technical analysis of system information assessing for vulnerabilities, threats and risks posed to the University.

Planning & Organising

- To assist, as deemed appropriate by the Cyber Security Architect, with the implementation and ongoing management of prevailing information and cyber security standards (e.g., ISO27001 & Cyber Essentials) including the gathering and preparation of information to support the certification processes.
- To research, evaluate, and assist in the deployment of technical solutions which help to protect the University's critical IT infrastructure.
- Support the development of architectural standards that are fundamentally secure.
- Assist in the development and improvement of:
    - Network and server hardening policies including deployment of an approved configuration management system.
    - Network vulnerability scanning and penetration testing.
    - Network and server event monitoring and compliance reporting.
    - Metrics to measure the overall Cyber Security risk to the University.
    - The Cyber Incident response plan and red team exercising.

Problem Solving

- To receive, classify, triage, and actively seek out suspected and actual security incidents in a time and cost-effective manner. This includes being a first point of contact for some incidents, working with other teams to record, classify and contain incidents as well as tracking security incidents to ensure closure within an appropriate timeframe.

Continuous Improvement

- To, in conjunction with the Cyber Security team and Information Governance team, develop and maintain the institutional education and awareness programme which aims to promote a culture of good cyber security practice throughout the University. This will include producing and maintaining content when needed and provide statistics on completion across the University.

	• To keep abreast of potential and emerging threats to the University's information systems, legislative and security framework changes and other IT activities. To assess the risks that the threats represent and to advise senior managers, system and service managers and other senior professional IT staff and managers as appropriate. • To measure that all security related processes and procedures adopted in all parts of the University are proportionate and sufficiently respectful of users' (staff and students) privacy rights and reasonable expectations. • To be an active member of the IT team, contributing to the development of department wide policies, processes and procedures. • To participate in University working groups and committees. The Cyber Security Officer is expected to contribute heavily on Cyber Security projects and initiatives as and when required.
Special Circumstances:	Work outside of normal hours, at weekends and during Public and University holidays may be required from time to time.

University of Sunderland

Role Profile

Part 2

lifechanging University of Sunderland

Part 2A: Essential and Desirable Criteria

Essential

Qualifications and Professional Memberships:

- Educated to degree level (or have equivalent level professional and practical experience).

Knowledge and Experience:

- Self-motivated with the ability to work with limited supervision.
- A good working knowledge of the ISO 27001 and Cyber Essentials security standards.
- Excellent organisational, prioritisation and time-management skills.
- Excellent problem solving and analytical skills.
- Demonstrable experience of working in IT in a similarly large and complex environment.
- The ability to maintain a rational and calm approach when working in highly pressurised situations.
- Collaborating with other colleagues, understanding their priorities and work commitments.
- The ability to work understand and interpret information from highly skilled, technical IT professionals.
- A detailed understanding of the theory and practice of cyber security.
- A good working knowledge of network protocols and internet technologies.
- A broad understanding of computer platforms e.g. Windows, Solaris and Linux.
- A broad understanding of cloud platforms e.g. Azure.
- A broad understanding of the law and accepted best practices especially around the prevailing data protection and computer misuse acts.
- An understanding of the principles and practices of cryptography.
- Experience of developing policies, procedures, and standards.
- High computer literacy skills including, but not exclusive to, Microsoft Office and online collaboration tools.

Desirable

Qualifications and Professional Memberships:

- One or more recognised professional qualifications in information security e.g. CISSP, CompTIA Security +.
- ISO 27001 Certified ISMS Foundation

Knowledge and Experience:

- A knowledge of computer forensics and familiarity with evidence handling best practices.
- A working knowledge of network data gathering tools, e.g. Wireshark or Nessus.
- Experience of working with auditors.
- Experience of conducting Information Security related risk assessments.

Part 2B: Key Competencies

Competencies are assessed at the interview/selection testing stage

COMMUNICATION

Oral communication

The role holder is required to, understand and convey straightforward information in a clear and accurate manner and the role holder is required to, understand and convey information which needs careful explanation or interpretation to help others understand, taking into account what to communicate and how best to convey the information to others and the role holder is required to, understand and convey complex conceptual ideas or complex information which may be highly detailed, technical or specialist.

Written or electronic communication and visual media

The role holder is required to, understand and convey straightforward information in a clear and accurate manner and the role holder is required to, understand and convey information which needs careful explanation or interpretation to help others understand, taking into account what to communicate and how best to convey the information to others and occasionally is required to, understand and convey complex conceptual ideas or complex information which may be highly detailed, technical or specialist.

INITIATIVE AND PROBLEM-SOLVING

The role holder is required to resolve problems where there is a mass of information or diverse, partial and conflicting data, with a range of potential options available; apply creativity to devise varied solutions, approaching the problem from different perspectives.

TEAM DEVELOPMENT

The role holder is required to advise or guide others working in the same team on standard information or procedures and the role holder is required to train or guide others on specific tasks, issues or activities; give advice, guidance and feedback on the basis of their own knowledge or experience; deliver training and the role holder is required to carry out training or development activity according to the needs of the individual or group; identify current capabilities and future needs; define the performance standards required; identify appropriate developmental activity; assess the application of learning; give feedback and guidance on overall performance.

SERVICE DELIVERY

The role holder is required to deal with internal or external contacts where the service is usually initiated by the role holder, working within the organisation's overall procedures or policies OR proactively seek to explore and understand customers' needs; adapt the service accordingly to ensure the usefulness or appropriateness and quality of service (content, time, accuracy, level of information, cost).

	DECISION-MAKING PROCESSES AND OUTCOMES The role holder is required to take independent decisions that have a moderate impact. The role holder is required to be party to some collaborative decisions; work with others to reach an optimal conclusion that have a significant impact. The role holder is required to provide advice or input to contribute to the decision-making of others that has a significant impact.
	KNOWLEDGE AND EXPERIENCE The role holder is required to apply a breadth or depth of experience showing full working knowledge and proficiency of their own area of expertise; act as a point of reference to others; demonstrate continuous specialist development, acquiring and refining skills and expertise in new or related areas through undertaking and encouraging internal or external development activity.
Date Completed:	January 2022