IT Security Analyst (Technical) - Learning & Information Services – Grade G

Job Description

Purpose

This role is a member of the IT Security Team and supporting the IT Security operations across the University. This specific role will work with departments, schools and third parties to support and provide oversight on the effectiveness of security controls across the university and third party systems, including technical assessments of incidents, vulnerabilities and compliance with technical polices and standards.

The IT Services teams ensure the University's user facing IT services continue to perform to the required levels of service, availability, security and flexibility, in support of the University's core business.

Working in close collaboration with the wider IT leads across the LIS Services, providing security expertise across all aspects of the University's IT estate, delivering a series of programmes and projects to ensure that systems are future proofed, applying appropriate governance, procurement and service management procedures, whilst maintaining regulatory, legal and professional standards.

The role holder will be key to ensuring the successful implementation of the University strategy for information and technology, supporting and providing modern, scalable and secure integrated platforms to support University business, including blended on-campus and online learning and teaching, research, administration, estate operations and commercial activity.

Duties

1. Provides a positive, supportive technical point of contact within a highly-performing team to deliver effective and efficient services, utilising modern processes to enable continuous performance improvement. Work collaboratively with team members to support the team and the wider department, ultimately the University meet their objectives.
2. Assist with the development of the university's technology vision and roadmap in collaboration with relevant stakeholders with a particular focus on Security. Provide technical expertise across the IT Security controls applied at the University.
3. Technical expertise in the set up and configuration of security logging across multiple technology platforms.
4. Technical expertise in the development and execution of the IT security malware detection, prevention and remediation process. Technical expertise in the development and execution of the IT security configuration benchmarks across multiple IT platforms.
5. Technical expertise in the development and execution of the IT security vulnerability management and issue remediation process, including execution of external and internal vulnerability scanning across all university networks.
6. Technical point of contact and technical expert for the security aspects of firewall management and network monitoring technologies and oversight on the effectiveness of network security management.

7. Lead the security incident management process and support the ongoing integration of incident management procedures across all areas of the university and strategic partners ensuring timely investigation of alerts and remediation activities.

8. Work across LIS and the University to provide significant contributions to development and implementation of the University's penetration testing/ethical hacking program including briefing LIS leadership and technical leads on issues found:

   In collaboration with the Governance Risk and Compliance IT Security Analyst.

- Provide technical security expertise and ownership in response to IT Service Management requests (Incidents / Requests / Problems / Changes) and lead the security aspects of LIS Projects in a timely manner.

- Continuously enhance the leading technology offering from the University to all its stakeholders by identifying and evaluating technology or productivity solutions.

- Ensure security features relating to the management of enterprise assets are embedded and effective.

- Ensure security features relating to software asset management are embedded and act as a key security contract for new software requests.

- Ensure Account management and access control reviews on critical infrastructure and systems are performed by technical leads and university stakeholders reporting control exceptions to IT security manager and LIS leadership members.

- Lead the execution of application security risk assessments and support the development and implementation of the application risk process across all stakeholders in the university. Undertake Application Security Risk Assessments.

- Lead the development and implantation of physical security standards and provide assurance over the implementation of physical security of IT systems and Assets.

- Lead the development of IT security standards and support the development of IT security polices including briefing of standards to senior technical stakeholders and technical compliance with related industry standards such as ISO27001, ISO22301, PCI-DSS, GDPR and NIST 800-53.

- Ensure mobile device management (MDM) and bring your own device (BYOD) facilities are developed and delivered from both a user experience, sustainability and also a security perspective.

9. Professionally represent LIS and collaborate with senior internal and external stakeholders to influence and steer the investments in infrastructure, software, and applications in support of the information & technology strategy contributing to relevant business cases.

10. Cooperate with colleagues across LIS to ensure knowledge, skills and resources are shared across the teams in support of strategic priorities, serving as a subject matter expert.

11. Where relevant to the skills of the role, lead the response and support audit requests and compliance against certifications such s as Cyber Essentials Plus, ISO 27001 and other similar requests.
12. Technical point of contact to produce IT security related management information and the operation of IT security controls, including contribution to the LIS and University Risk Registers.
13. Support and deputise for Governance, Risk and Compliance Security Analyst.
14. Demonstrate flexibility and commitment to the University strategic and development plans.
15. Staff may be required, from time to time and on an ad hoc basis, to work additional hours and/or hours outside of their normal working pattern to meet the needs of the business including provide emergency response out of hours.
16. To observe, monitor and comply with all relevant University policies and procedures in the performance of duties, particularly in relation to System and Information Security.
17. Undertake any other duties commensurate with the grade of the role, deputise for the Head of IT services and Operations or IT Security Manager upon request.

Knowledge, Skills, and Behaviours (Essential)

- Experience in IT security or IT technical roles, handling various responsibilities, including creating high-level plans and working with success measures aligned to institutional metrics or targets (Application/Interview).
- Proven ability to communicate, influence, and represent technical leadership in both external and internal meetings and forums (Application/Interview).
- Skilled in dealing with demanding customers and embedding a culture of service within teams (Application/Interview).
- Proficient in investigating problems and resolving issues ensuring the confidentiality, integrity and availability of business systems is fit for purpose (Application/Interview).
- Experienced in data analytics, statistical analysis, and supporting IT services across in-house, third-party, and cloud-based platforms (Application/Interview).
- Relevant business or systems-based undergraduate degree or equivalent work experience (Application).
- Exceptional communication, collaboration, and people skills. Capable of engaging colleagues and stakeholders at all organizational levels, regardless of technical expertise, with great listening, empathy, insight, and intellect. (Application/Interview).
- Excellent communication and collaboration skills – verbal and written – with the ability to talk and present to colleagues and stakeholders at all levels of an organisation with varying technical experience and capabilities (Application/Interview).
- Credibility to effectively engage with senior professional and academic colleagues, sector-leading suppliers and external stakeholders. A high level of communication, negotiation and influencing skills (Application/Interview).
- Strong problem-solving skills with ability to gather and assimilate information (Application/Interview).

- Ability to remain calm and work well under pressure, both as part of the team and on own initiative (Application/Interview).
- Ability to think ahead and anticipate/mitigate risks and find suitable solutions to issues (Application/Interview).
- An understanding of and demonstrable commitment to the University's Values of Achieving Together, Supporting all, Being Proud and Creating Opportunity, as a framework for decisions, actions and behaviours (Application/Interview).

Knowledge, Skills, and Behaviours (Desirable)

- Experience of working in leadership within the UK education sector (Application/Interview).
- Experience of leading and operating within an Agile, Service Managed environment (Application/Interview).
- Experience of writing, process and policy documents, and cases for support (Application/Interview).
- Relevant Technology-based certifications and or Recognised ITIL qualification (Application).
- Recognised Project Management and Agile process qualifications and or a recognised IT or/or business leadership qualification (Application).
- Experience of public sector procurement processes, strategic IT vendor management and strategic partnership development including contract management (Application/Interview).