JOB DESCRIPTION

Vacancy reference:	SRF34452
Post Title:	Junior Security Engineer
Grade:	5
School/Department:	Digital Technology Services (DTS)
Reports to:	Infrastructure Manager or Cloud Manager
Responsible for:	N/A

Purpose

Digital Technology Services supports the University of Reading with centralised IT infrastructure and an important component is the provision of high-quality network services and management of all local and wide area network connections, fixed-line voice networks, associated hardware, software, and communication infrastructure.

The IT Security Team ensures the confidentiality, integrity, and availability of information assets.

The role of Junior IT Security Engineer is to support and maintain these services under the guidance of the team manager and other engineers in the team.

Main duties and responsibilities

Technical execution

1. Work with the IT Security Team to identify improvements to IT Security policies and procedures which can be used by others within DTS
2. Monitor the day-to-day compliance of security controls
3. Contribute ideas to improve information security standards, procedures, and processes.
4. Review and identify actions from regular security testing against new and existing services.
5. Support the day-to-day monitoring of services, analysing and interpreting outputs to identify security weaknesses
6. Support upgrades to services in and out of projects.
7. Provide a point of contact on sensitive matters such as investigations and audit reports and resolving queries promptly and confidentially
8. Be responsible for the triage of incidents and requests being raised into the security team and escalate to IT Security Engineers and Management as appropriate.
9. Ensure that customer requests in the areas of service responsibility are handled promptly and effectively such that agreed service levels are met
10. Ensure that operational processes and facilities relating to the core services are accurately documented, maintained, and reviewed regularly to ensure their effectiveness and efficiency

Technical oversight

11. Propose the development of service improvements
12. Support the production of monthly reporting of KPIs, performance of service area and other management information as agreed with the Head of Operations
13. Contribute to a continuous service improvement plan for existing services and work with the Head of Operations to provide a roadmap of development activity

14. Take a lead role in supporting the Service Desk with incident troubleshooting and issues resolution, identifying, and remedying performance bottlenecks and managing incidents, problems and ensuring that communications between the Service Desk and the Security Team are effective
15. Support the work with senior stakeholders to schedule and undertake maintenance on core systems and services to ensure that they are secure, fit for purpose and able to meet the demands of users
16. Provide support and guidance of policy and process to customers so they understand their requirements to improve services ensuring that complex problems are understood, communicated, and resolved

Professional standards

17. Keep up to date with information security regulations and policy effecting services, such as The Data Protection Act 2018 (including GDPR), FOI and RIPA
18. Engage with staff in similar positions in other HE institutions to share good practice
19. Keep up to date with current industry good practice and trends in IT service provision

Supervision received

The post holder will report to the Infrastructure Manager or Cloud Services Manager and will be expected to work with some supervision. The post-holder and manager will agree objectives as appropriate. They will be expected to manage their own time to complete the work that they have been set by their manager to meet the requirements and objectives for the post.

Supervision given

This role is not expected to provide a specific supervision.

Contact

There is regular and frequent contact business service teams within the University and the suppliers and manufacturers of the various applications. This may include involvement in procurement, tenders, requesting technical assistance, requesting consultancy, raising support queries and escalation of outstanding issues.

It is expected that the post holder will have contacts with staff with similar responsibilities at other HE institutions through national email lists and attendance at relevant events.

Terms and conditions

Full time, permanent role. Flexibility will be required to ensure that service is maintained within normal working hours. Planned maintenance is scheduled for Tuesday evenings wherever possible with time off in lieu available for such working.

The post holder may be required to be onsite or be on call for specific events or when a critical or major incident occurs. Additional payments will apply in these circumstances.

This document outlines the duties required for the time being of the post to indicate the level of responsibility. It is not a comprehensive or exhaustive list and the line manager may vary duties from time to time which do not change the general character of the job or the level of responsibility entailed.

Date assessed: December 2020

PERSON SPECIFICATION

Job Title	School/Department
Junior Security Engineer	Digital Technology Services

Criteria	Essential	Desirable
Skills Required	• Understanding of security systems and services • Ability to prioritise competing and complex work demands • Excellent communication skills including presentation of technical issues for non-specialist audiences • Ability to take innovative approaches to problem solving. • Ability to work effectively under pressure. • Ability to create clear and concise documentation	• Exposure to supporting Cloud service such as Azure and Office 365 • Technical knowledge of Windows, Linux and macOS
Attainment	• IT background through education, work, and ability to talk about experience. • Educated to degree level or able to demonstrate an equivalent level of professional learning and development	• Advanced security certification (e.g., CISSP or CRISC) • ITIL Foundation
Knowledge	• Experience in building and maintaining security systems in an enterprise environment • Technical background with exposure to security, network, or cloud infrastructure administration • Working knowledge of various security technologies such as: Active Directory, Anti-malware protection, Vulnerability Scanners, intrusion detection/prevention, system hardening • Knowledge of directory technologies (e.g. AD, DNS)	• Knowledge of the principles of Penetration Testing and Security Scanning • Knowledge of Virtualisation Technologies and Hypervisors • Knowledge of security frameworks (e.g., Cyber Essentials or ISO27001) • Management of high availability IT • Security knowledge of a wide variety of IT systems such as operating systems (Microsoft, Unix/Linux), email (Exchange), Unified Messaging (Teams)

Relevant Experience	• Understanding of securing core centralised storage, server, and services within a large and complex environment • Experience of managing small projects	• Experience of providing multiple services to agreed levels. • Experience of working in a public sector or Higher Education environment • Experience of procurement rules and processes • Experience in working with suppliers and partners • Management of high availability IT Core Systems • Experience of delivering services to mobile devices
Disposition	• Commitment to the values of the University • Evidence of continuing personal development and training • Commitment to staff development and support	

Completed by: Kevin Mortimer Date: 6/12/2020