ID: J60

College/Service: **Exeter IT**

Post: **Operations & Security Manager**

Reference: **P58857**

Grade: **G**

Reporting To: **Assistant Director – Service Management**

Responsible For: **Security and Incident & Service Improvement Teams**

ORGANISATIONAL CONTEXT

The University of Exeter is a Russell Group university that combines world-class research with very high levels of student satisfaction. Our vision is to become one of the most successful universities in the world, one that makes the exceptional happen by challenging traditional thinking and defying conventional boundaries.

IT SERVICE

Exeter IT is a key enabler for this vision and is key to delivering the University's Values and its world class reputation. The IT & Digital strategy will support the growing ambitions for education, research and professional services, and exploiting the opportunities from changing technology will enable the University to thrive in an increasingly digital environment.

What makes Exeter IT different is its defining characteristics: *strong leadership*, *active collaboration, forward thinking, and delivering at pace*. We expect our staff to be comfortable with responsibility, and be innovative and creative in the delivery of IT and digital services. Being able to adapt to the momentum of change and having the freedom of action will enable staff to deliver IT solutions that will have a positive impact on our students, academics, and professional services staff.

SERVICE MANAGEMENT

The changing digital technology landscape and increase in SaaS and other emerging technologies requires a wide range of new skills in the IT service. Service Management covers a broad range of functions and capabilities to deliver a service that is completely customer focussed, service centric and design led. The IT strategic objectives are realised through Service Management, and requires effective and efficient delivery and support of IT services to ensure value for education, research and professional services. Service Management functions and capabilities are critical to manage IT services at agreed levels and for the ongoing management of the live hybrid environment of on-premise, legacy and cloud applications, data and hardware that are used to deliver and support services.

IT OPERATIONS & SECURITY

The IT Operations and Security function will ensure high levels of business satisfaction and confidence in IT. It will manage the effective response to incidents and problems, ensuring the delivery of IT services to agreed service levels whilst balancing stability and responsiveness with quality and cost of service, and proactively looking for ways to improve.
The function will also develop and implement cybersecurity tools, processes and practices designed to protect networks, computers, programs and data from attack, damage and prevent unauthorised access.

Reporting Structure

For the reporting structure of this job, please see the attached structure chart.

Main purpose of the job

Lead the Operations & Security teams that are responsible for ensuring the enforcement of the IT cybersecurity policies and working practices, and prioritising and analysing problems and root causes of recurring incidents
You will be responsible for the major incident and significant event process and will ensure incidents are investigated, analysed and reported, establishing the relevant team to concentrate on speedy resolution.

The Operations & Security teams will flex in size depending on demand.

Key accountabilities

1. Support the Assistant Director Service Management and coordinate the monitoring, analysis and reporting of the end-to-end performance of all IT services to ensure operational and service levels are met and improved, and aligned with business service value.
2. Support the Assistant Director Service Management and help manage the governance of high severity incidents and events across the IT service supply chain to minimise disruption and focus IT staff and technical experts to concentrate on speedy resolution.
3. Support the Assistant Director Service Management and coordinate the defence against cyber-attacks and unauthorised access including identifying vulnerabilities, and attack prevention and detection, ensuring work is coordinated to anticipate risk, mitigate, recovery and restore services.
4. Implement complex operational, security and problem solving activities for IT and Digital services applying a wide range of business, technical and management principles, and provide professional advice about your area of expertise to inform decision making that impacts resourcing and future business planning of the service.
5. Provide leadership and be accountable for the performance of processes and systems where the role is the Process or Systems Owner, and contribute to strategy and policy formulation for your area of specialism, communicating the impact of any changes to IT services to the business.
6. Convey the value of complex conceptual IT operations and security services through written, verbal and visual communications to senior stakeholders, and lead on the evaluation of new software products and digital services in support of developing the business case for change.
7. Accountable for managing resources, setting measurable goals and performance targets for your team, including driving service improvement to meet customer's needs, delivering results and report against these to demonstrate progress, and ensure effective productivity of staff and quality delivery of outputs.
8. Manage and be responsive to the changing or conflicting demands on your team by utilising budgeted resources, leveraging different delivery methods and techniques, negotiating with key stakeholders, and be responsible for managing operational budgets when delegated to the role.
9. Lead and manage projects when required and be responsible for the time, cost and quality of deliverables including managing project budgets. Actively participate in University projects and working groups where appropriate.
10. Accountable for the identification and implementation of service improvement opportunities to drive down demand and increase efficiency without sacrificing customer satisfaction, ensuring all processes are standardised and documented with supporting process controls.
11. Overall responsibility for the efficient and professional approach to managing reported incidents to ensure user satisfaction with the quality of IT services is maintained.
12. Overall responsibility for the effective analysis of problems and root causes to prevent problems and resulting incidents from happening, eliminate recurring incidents, and minimise the impact of incidents that cannot be prevented.
13. Overall responsibility for the maintenance and availability of reliable knowledge and information to support all IT service activities, and improve efficiency by reducing the need to rediscover knowledge.
14. Responsibility for the presence on supplier forums and events to identify future opportunities to improve IT security and incident management.
15. Manage the quality and timeliness of deliverables from contractors and vendor resources, and line manage fixed term staff when appropriate.
16. Responsible for mentoring and coaching team resources and deliver training on your area of expertise.

17. This job description summarises the main duties and accountabilities of the post and the post-holder may be required to undertake other duties of similar level and responsibility including deputising for your line manager.

The post holder will be required to provide support across all University campuses, and may be required to work additional hours to meet the requirements of the role.

All Exeter IT staff are expected to:

- Ensure the seamless and integrated end-to-end service delivery to academic, research and professional services staff.
- Be passionate about new IT and digital technologies, and promote and be an advocate for the IT operating model and IT & Digital strategies.
- Work closely with the Continual Service Improvement capability to ensure IT services are aligned to current and future business needs, and identify opportunities to improve efficiency and effectiveness in the IT services are delivered.
- Work closely with the Knowledge Management capability to share perspectives, ideas, experience and information to support decision making and manage IT services.
- Raise the positive profile and good reputation of the University and contribute as a member to your IT networks and engagements, both locally and nationally where appropriate to the role.
- Proactive personal and professional development including completion of mandatory training, skills courses and specialist training.
- Professionally represent the IT service by adopting the dress code or uniform appropriate to your role.

Skills Framework for the Information Age (SFIA)

IT roles at the University of Exeter have been mapped to the industry good practice Skills Framework for the Information Age (SFIA[1]).The role is mapped as a SFIA level 6 *"Initiate, influence"* against the core competencies *autonomy, influence, complexity and business skills*, and summarised as:

Autonomy

Has defined authority and accountability for actions and decisions within a significant area of work, including technical, financial and quality aspects. Establishes organisational objectives and assigns responsibilities.

Influence

Influences policy and strategy formation. Initiates influential relationships with internal and external customers, suppliers and partners at senior management level, including industry leaders. Makes decisions which impact the work of employing organisations, achievement of organisational objectives and financial performance.

Complexity

Has a broad business understanding and deep understanding of own specialism(s). Performs highly complex work activities covering technical, financial and quality aspects. Contributes to the implementation of policy and strategy. Creatively applies a wide range of technical and/or management principles.

Business skills

Absorbs complex information and communicates effectively at all levels to both technical and non-technical audiences. Manages and mitigates risk. Understands the implications of new technologies. Demonstrates clear leadership. Understands and communicates industry developments, and the role and impact of technology in the employing organisation. Promotes compliance with relevant legislation. Takes the initiative to keep both own and colleagues' skills up to date.

Most commonly identified specific SFIA skills required for the role are:

GOVN	IT governance
IRMG	Information management
SCTY	Information security
INAS	Information assurance
CNSL	Consultancy

[1] http://www.sfia-online.org/en

TECH Technical specialism
BPRE Business process improvement
BURM Business risk management
PRMG Project management

Person Specification

Competency	Essential	Desirable
Qualifications and attainment	• Educational attainment at degree level (or demonstrable equivalent experience) • ITIL ® Foundation	• Industry standard IT related certification or professional qualification including: • Degree in Computer Science • Degree in Cyber Security • ISO 27000 • Information security certification (e.g. CISSP, CISM, CCP) • Prince 2 or equivalent
Knowledge & skills	• Excellent methodical, analytical (qualitative and quantitative) and problem-solving skills • Excellent planning and organisational skills • Strong communication skills demonstrating the ability to convey the value of complex conceptual ideas and new technologies to senior stakeholders • Proven ability in negotiation and influencing stakeholders at senior management level in a matrix environment • Ability to prioritise and organise work of others and ensure effective use of resources within your own area to overcome conflicting demands. • Ability to set objectives and action plans for others in the team and monitor and report performance. Capable of independently assessing the impact of increasing demand and be proactive in undertaking activities to resolve the situation	
Prior experience	• Experience of managing information security, including threats, attacks, and vulnerabilities. • Experience of managing major incident and significant event processes including the investigation, analyses and speedy resolution. • Proven leadership experience and managing teams in a matrix environment, setting performance standards and targets, creating communities, and motivating others	• Experience of working in the Higher Education sector. • Experience of working in a Design, Develop, Operate environment • Experience of working in a SIAM environment. • Experience of developing business cases for change to deliver organisational benefit

	• Experience of managing competing demand and priorities. • Successful management of budgets and human resources in response to changing or conflicting demands • Experience of managing organisational change within a team • Experience of monitoring service performance and driving continual service improvement • Experience of developing influential relationships with external partners and suppliers • Proven experience of managing relationships within teams, evidencing ability to break down barriers and building beneficial working relationships • Demonstrate experience of anticipating problems and making projections that impact the strategic direction of the service • Proven experience of undertaking complex analysis, using different methodologies, and providing reports and management information with supporting commentary • Experience in the identification and proactive mitigation of risks	• Member or participant in local and national IT networks and communities
Behaviours	• Thrive in an environment of change, demonstrating flexibility and adaptability • Comfortable with responsibility and freedom to take action • Take responsibilities for actions, identify and implement subsequent lessons learnt • Demonstrate a proactive and positive approach to problem-solving, suggesting innovative and workable solutions both at strategic and operational level. • Demonstrate continuous professional development • Work effectively and collaboratively as part of a senior team in a matrix environment • Be resilient, retaining composure under pressure	

Circumstances	• Provide support across all University campuses • May be required to work additional hours to meet the requirements of the role	

Terms & Conditions
Our Terms and Conditions of Employment can be viewed here.

Further Information
Please see our website for further information on working at the University of Exeter.