College/Service: **Exeter IT**

Post: **Head of IT Security & Compliance**

Reference: **P58847**

Grade: **G**

Reporting To: **Assistant Director – Strategy & Architecture**

Responsible For: **IT Security & Compliance capability**

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.

THE 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.

STRATEGY & ARCHITECTURE

The changing digital technology landscape and increase in SaaS and other emerging technologies requires a wide range of new skills in the IT service. Strategy & Architecture covers a broad range of functions and capabilities to deliver a service that is completely customer focussed, service centric and design led. Strategy & Architecture also helps to define the relationship between the various IT services, systems and processes to deliver the University strategies and business plans. The innovative use of IT and digital services including enterprise architecture, IT security, and a portfolio and catalogue of IT services, is designed to meet current and future University services and business processes.

IT SECURITY & COMPLIANCE

The IT Security & Compliance function will develop robust information security, risk management, and audit and compliance strategies supported by appropriate methodologies to protect the University's IT systems and information assets, and to meet regulatory and legal obligations as well as academic and professional services expectations.

Main purpose of the job

Establish and lead the IT Security & Compliance capability that develops the strategy, policies and procedures for information security, risk management, audit and compliance to protect the University's IT systems and information assets, and to meet regulatory and legal obligations as well as academic and professional services expectations.

Key accountabilities

1. Support the Assistant Director Strategy & Architecture and the University's Governance & Compliance Office in the development and enforcement of security policies, standards and practices, and assessing all aspects of technical and security risks and the business impact, and ensure vulnerable information is acted upon.
2. Accountable for the integrity, availability, authenticity, non-repudiation and confidentiality of information and data, including overall responsibility for the classification of information assets and documentation.
3. Accountable for setting measurable goals and performance targets, delivering results and report against these to demonstrate progress, and manage the activities and tasks allocated to staff to ensure effective productivity and quality delivery of outputs.
4. Manage and be responsive to the changing or conflicting demands 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.
5. Lead, and be accountable for, the performance of processes and systems, and contribute to strategy and policy formulation.
6. Responsible for establishing an enterprise security stance through policy, architecture and training processes.
7. Overall responsibility for investigating major breaches of security and recommending appropriate control improvements.
8. Lead on the security accreditation of complex information systems utilising industry assurance methods, techniques and certifications.
9. Overall responsibility for risks management including the IT service risk register, liaising with internal and external auditors, and sponsoring risk mitigation or remediation projects to minimise the vulnerabilities and threats with technology.
10. Drive the automation of internal controls and the central logging and reporting of risks to improve the effectiveness of risk management and support better decision making.
11. Coordinate and lead on periodic audit reviews for new suppliers, IT services, technologies and processes to ensure that security objectives are enforced.
12. Coordinate and lead on the deployment, integration and configuration of all new security solutions and enhancements to existing solutions.
13. Maintain up-to-date knowledge of the IT security industry and of compliance regimes including awareness of new or revised security solutions, and the development of new attacks and threat vectors.
14. Responsible for developing and delivering training and providing professional advice about your area of expertise or where there are new developments in technology.
15. Lead and manage small/medium projects when required and be responsible for the time, cost and quality of deliverables including managing project budgets. You will actively participate in University projects where appropriate.
16. Responsible for mentoring and coaching team resources, deliver training, and provide professional advice about your area of expertise.
17. Provide leadership and be accountable for the performance of processes and systems where the role is the Process or Systems Owner.

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.
- 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 and 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
SCTY	Information security
INAS	Information assurance
CNSL	Consultancy
TECH	Technical specialism
SCAD	Security administration
QUAS	Quality assurance

Person Specification

Competency	Essential	Desirable
Qualifications & attainment	• Educational attainment at degree level (or demonstrable equivalent experience)	• Industry standard IT related certification or professional qualification including: • ISO 27000

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

	• Risk Management IT frameworks • Information security certification (e.g. CISSP, CISM, CCP,GIAC) • ITIL ® Foundation	• COBIT governance & management framework • Detailed knowledge of the regulatory framework for information security including the Data Protection Act, and the Freedom of Information Act
Knowledge & skills	• Knowledge of the standards pertaining to the area of Information Security, such as ISO27001/2, Cyber Essentials, PCI-DSS. • Excellent understanding of IT and digital systems and their vulnerabilities • Proven ability in assessing and managing risks • Proven ability in information security management • Excellent methodical, analytical (qualitative and quantitative) and problem-solving 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 • Proven ability to take independent decisions relating to significant events or influence decision making that impacts resourcing and future business planning of the service • 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	• Recent significant experience in information security management and/or related functions (such as IT audit and IT Risk Management) in a commercial environment, demonstrating business acumen, balancing financial, quality, people and customer expectations	• Project Management methods, processes, tools and techniques. • Experience with IPS/IDS and SIEM technologies. • A background in technical IT roles such as IT architecture, development or operations, with a clear and

	• Proven leadership experience and managing teams in a matrix environment, setting performance standards and targets, creating communities, and motivating others • Successful management of budgets and human resources in response to changing or conflicting demands • Experience of managing organisational change within a team • 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	abiding interest in information security. • Experience of working in a Design, Develop, Operate environment • 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 • Work in a no-blame culture, taking responsibilities for actions, and learning lessons • 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.