JOB DESCRIPTION

JOB TITLE	Information Security Manager				
DEPARTMENT	ICT				
JOB NUMBER		**GRADE**	7	**DATE**	
REPORTS TO	Security, Compliance and Administration Manager				

CONTEXT

JOB PURPOSE

This position sits within the central security, compliance and administration team of ICT Services but has a remit across the department as a whole. Reporting to the Security, Compliance and Administration Manager the role is responsible for the development, delivery, and enforcement of comprehensive information security arrangements. Security and compliance run through every aspect of the operation of the ICT department, and it is essential that the operation of all ICT services is delivered in a manner that protects the University and in particular protects all personal and confidential data and information. The delivery of ICT services and operation of the ICT department must also comply with all relevant regulations and legislation.

The post holder will liaise with technical specialists within ICT and other departments to agree appropriate security measures to ensure confidentiality, integrity and availability of university systems and data. The post holder will take the lead and provide a focal point for security and information risk matters.

The post holder will be required to advise and offer guidance on existing security arrangements and be actively involved in the specification, design and implementation of new services.

The post holder must ensure that they keep up to date with developments in best practise, standards, and technologies within the sector and beyond.

Autonomy
Works under broad direction. Work is often self-initiated. Is fully accountable for meeting allocated technical and/or project/supervisory objectives. Establishes milestones and has a significant role in the delegation of responsibilities.

Influence
Influences organisation, customers, suppliers, partners and peers on the contribution of own specialism. Builds appropriate and effective business relationships. Makes decisions which impact the success of assigned projects i.e., results, deadlines, and budget. Has significant influence over the allocation and management of resources appropriate to given assignments. This role is expected to be a role model to others across the department.

Complexity
Performs an extensive range and variety of complex technical and/or professional work activities. Undertakes work which requires the application of fundamental principles in a wide and often unpredictable range of contexts. Understands the relationship between own specialism and wider customer/organisational requirements.

Business Skills
Advises on the available standards, methods, tools and applications relevant to own specialism and can make appropriate choices from alternatives. Analyses, designs, plans, executes and evaluates work to time, cost and quality targets. Assesses and evaluates risk. Communicates effectively, both formally and informally. Demonstrates leadership. Facilitates collaboration between stakeholders who have diverse objectives. Understands the relevance of own area of responsibility/specialism to the employing organisation. Takes customer requirements into account when making proposals. Takes initiative to keep skills up to date. Mentors' colleagues. Maintains an awareness of developments in the industry. Analyses requirements and advises on scope and options for continuous operational improvement. Demonstrates creativity and innovation in applying solutions for the benefit of the customer/stakeholder. Takes account of relevant legislation.

KEY RESPONSIBILITIES

Strategy, Standards, Policy and Procedure

Develops information security policy, standards, and guidelines appropriate to business, technology, and legal requirements and in accordance with best professional and industry practice (PCI-DSS, GDPR, DPA, FOI etc.).

Ensure regular reviews of policy documents are conducted. Advising the Security group of proposed changes before obtaining sign-off.

Prepares and maintains a business strategy and plan for information security work which addresses the evolving business risk and information control requirements, and is consistent with relevant IT and business plans, budgets, strategies, etc.

Contributing to the ICT Services business continuity planning, the University IT disaster recovery Planning strategy and architectural standards.

Compliance and Enforcement

Carry out regular ICT security audits both internal and with the assistance of external security specialists. Regular inspections of systems and functions to ensure compliance with university policy and to ensure that any gaps are filled.

To ensure any remedial actions are carried out in an effective and timely manner.

Conducts security control reviews across a full range of control types and techniques, for business applications and computer installations; both internally generated and in conjunction with external security specialists. Recommends appropriate action to management to ensure any identified gaps are filled.

Provides authoritative advice and guidance on the application and operation of all types of security controls, including legislative or regulatory requirements such as data protection and software copyright law.

Evaluates the storage, transmission, sharing, publishing, and handling of university data across all relevant systems. To implement best practice to ensure security, whilst maintaining business needs, through the application of formal protection measures.

Conducts investigation, analysis and review following breaches of security controls, and manages security incidents. Prepares recommendations for appropriate control improvements, involving other professionals as required.

Devises and implements document and record systems, including classification, security, retrieval, and retention processes.

Manages the operation of appropriate security controls as a production service to business system users.

Risk Assessment and Contingency Planning

Conduct Information security Risk assessments: suggest and advise on realistic measures to mitigate any identified risks. Maintenance and development of an existing set of KPI's that measure the current threat level and effectiveness of security University measures as well as providing information to aid in prioritisation and decision making.

Identifies and manages assessment of threats to confidentiality, integrity, availability, accountability, and relevant compliance. Takes ownership of security control reviews, business risk assessments, and reviews that follow significant breaches of security controls.

Contribute to both the local ICT Risk register and the overall University risk register where appropriate.

To investigate suspected and actual security incidents in accordance with the security incident management standard, produce reports with recommendations and ensure any remedial action is taken.

To work closely with colleagues across the department to develop and maintain ICT disaster recovery measures and to play a role in the University Business Continuity planning exercises.

Communication

Operates as a focus for IT security expertise for the University, providing authoritative advice and guidance on the application and operation of all types of security control, including legislative or regulatory requirements such as data protection and software copyright law.

Regular reporting of Security matters to the ICT management team.

Offering advice and guidance at all levels to ICT staff and individuals across the University.

To act as a respected champion of ICT security, promoting best practices within ICT Services and the University as a whole. Maintain, develop, and enact a comprehensive information security communications plan designed to inform and educate all staff and students within the University.

To promote security awareness by developing, implementing, and delivering a security awareness and training programme. Delivers and contributes to the design and development of specialist IT security education and training to IT and system user management, staff, and students.

Foster key relationships with internal stakeholders to help promote and improve information security and provide security advice on procurements, projects and new initiatives as required.

Project Management

To lead on Security focused projects ensuring that the ICT project management methodologies are followed.

To act as a trusted advisor on all projects that involve the securing of university data.

Plans and manages the work of small teams of staff on complex IT security specialism projects.

Manages the work of other IT specialist staff, including project and task definition and prioritisation, quality management and budgetary control, and management tasks that pertain to information security.

Other Responsibilities & Duties

Develops and maintains knowledge and communicates the information security and compliance by:

- Reading relevant literature and attending training.
- Attending conferences and seminars, meeting and maintaining contact with others involved in the technical specialism and through taking an active part in appropriate professional and trade bodies.
- Maintains an awareness of current developments in broad technical areas and takes significant responsibility for own personal development.
- Provides specialist guidance and advice to less experienced colleagues and users to ensure that work is conducted in an appropriate manner.

Champions the benefits of technical specialism and plays a leading role in special interest groups concerned with the technical specialism and writes, or contributes to, articles and papers and speaks at conferences, user groups, or specialist subject groups.

Communicates well, both orally and in writing, and responds to wide-ranging and detailed questioning relating both to own areas of specialisation and, at a more general level, to the wider field of IT both orally and in writing.

Promotes the service within the University and creates strong personal relationships with the full range of senior stakeholders.

Liaises with HE sectors and external organisations and key suppliers to share ideas, compare approaches and develop best practice.

In addition to the above, undertake such duties as may reasonably be requested and that are commensurate with the nature and grade of the post.

ADDITIONAL INFORMATION

Scope and Dimensions of the Role

The post holder will work flexibly, independently of location, in order to deliver on objectives.

Key working relationships/networks	
Internal	**External**
Director and Deputy Directors of ICT Security, Compliance and Administration Manager Infrastructure Manager and team AV & Operations Manager and team Service Desk Manager and team Head of Architecture and Programmes and team Information Services Managers and team Information Compliance Officers Staff at all levels within the university Students	Software, hardware, and service suppliers; including sales and technical support. Jisc CiSP Other Relevant HE sectors and national security organisations ICT staff in other institutions

PERSON SPECIFICATION

JOB TITLE	Information Security Manager	**JOB NUMBER**	

Selection Criteria	**Essential (E) or Desirable (D)**	**Where Evidenced Application (A) Interview (I) Presentation (P) References (R)**
Qualifications:		
Educated to degree level or equivalent experience	E	A,I
Relevant industry qualifications (e.g. CISSP, CISM, ITIL, etc.)	D	A,I
Membership of relevant professional bodies	D	A,I
Experience:		
Demonstrable relevant experience in methods and techniques for risk management, business impact analysis, countermeasures and contingency arrangements.	E	A,I
Demonstrable experience in the principles, practices, tools and techniques of IT auditing.	E	A,I
Experience of working in a large, challenging multi-site service delivery environment	E	A,I
Experience of solution development, design and review.	E	A,I
Experience of penetration testing	E	A,I
Demonstrable success in deploying methods and techniques for preparing and presenting business cases, invitations to tender and statements of requirements.	D	A,I
Demonstrable experience of working within agreed budget, timescales and resources to deliver successful outcomes.	E	I,R
Knowledge of the HE sector	D	A,I
Skills and Knowledge:		
Specific skills & knowledge of information security, data protection, compliance, related legislation and regulations	E	A,I
Shows aptitude for analysing and managing problems arising from incidents in the operation of information systems combined with the ability to provide innovative technical solutions.	E	A,I
Technical investigation skills, the ability to research and collate information from a wide variety of sources into technical reports and recommendations.	E	A,I
Excellent written and verbal communication skills, Able to present to a wide range of audiences ranging in knowledge of technology, business awareness and seniority	E	A,I
Supplier Relationship Skills	E	A,I
Relevant issues and trends in security management	E	A,I

Relevant issues, developments and trends within the education sector	D	A,I
Competencies and Personal Attributes:		
Credibility and integrity	E	I,R
Positive and open in communication both verbal and written	E	I,R
Initiative and confidence	E	A,I,R
Commitment to service quality	E	A,I
Analytical in approach to acquiring knowledge and information	E	A,I
Collaborative, able to build working networks	E	A,I,R
Commitment to service quality whilst adhering to internal procedures.	E	A,I,R
Desire to undertake further personal development and training.	E	A,I
Ability to assimilate technical information and keep up to date with emerging and developments in technologies, best practices and standards.	E	A,I

Essential Requirements are those, without which, a candidate would not be able to do the job. **Desirable Requirements** are those which would be useful for the post holder to possess and will be considered when more than one applicant meets the essential requirements.