UEL University of East London
Professional Services

JOB DESCRIPTION

Job Title:	Information Security & Compliance Manager
Grade:	F
School/Service:	IT Services
Campus:	Docklands
Responsible to:	Head of Service Management
Responsible for:	TBC
Liaison with:	Legal & Governance Services, Marketing & Communications, Head of Data Protection & Compliance, Strategic Planning and external relevant bodies such as UCISA, PCI-DSS, Information Commissioner’s Office etc.

JOB PURPOSE:

The Information Security & Compliance Manager (ISCM) role is a critical role in the CIO’s team. The role holder will work to deliver the objectives within the University Information Security strategy and further enhance a security program that identifies and addresses security and privacy risks and security requirements. The ISCM will be responsible for managing the process of gathering, analysing & assessing the current & future information security and privacy threats to the University as well as maintain & monitor the information security best practices as they develop.

The role holder will work with senior managers across the university to drive the information security agenda and ensure that it meets complex compliance requirements. They will act as an empowered representative of the CIO during IT planning initiatives to ensure that security controls are incorporated into IT projects at the design stage and expectations are clearly defined. The role holder will also play a key role in the evaluation of current Information Security breach management processes and ensure that the university can meet its mandatory data breach notification obligations should the need arise.

MAIN DUTIES AND RESPONSIBILITIES:

Strategic Support

1. Work with the CIO and senior managers to build on an existing information security program and ongoing security projects that address information security risks and compliance requirements.

2. Manage the process of gathering, analysing and assessing the current and future threat landscape, as well as providing the CIO & senior managers with a realistic overview of risks and threats in the enterprise environment.

3. Lead the preparation of institutional Information Security audits.

4. Monitor and report on compliance with security policies, as well as the enforcement of policies across the university.

5. Evaluation of compliance with stakeholder requirements, including response to requirement specifications from potential funders such as research councils & government departments.

6. Evaluate and update to new & existing policies and procedures to ensure operating efficiency and regulatory compliance.

7. Work as part of the General Data Protection Regulation Steering Group to ensure that the University can meet Information Security requirements under the Regulation and fulfil the array of data subject rights.

Architecture / Engineering Support

1. Consult with IT colleagues to ensure that security is factored into the evaluation, selection, installation and configuration of hardware, applications and software as part of Privacy by Design and Default.

2. Recommend and coordinate the implementation of technical controls to support and enforce defined security policies.

3. Research, evaluate, design, test, recommend or plan the implementation of new or updated information security hardware or software, and analyse its impact on the existing environment; provide technical and managerial expertise for the administration of security tools.

4. Develop a strong working relationship with the CIS, Infrastructure, WEB and other ITS teams to develop and implement controls and configurations aligned with security policies and legal, regulatory and audit requirements.

Operational Support

5. Manage and coordinate operational components of security incident management, including detection response and reporting.

6. Manage the day-to-day activities of threat and vulnerability management, identify risk tolerances, recommend treatment plans and communicate information about residual risk.

7. Manage security projects and provide expert guidance on security matters for other IT projects.

8. Evaluate requests for exceptions to policies, ensuring sufficient mitigating controls are in place.

9. Ensure audit trails, system logs and other monitoring data sources are reviewed periodically and are in compliance with policies and audit requirements.

Liaison & Networking – Information Security Liaison

10. Provide Information security communication, awareness and training to the appropriate university staff and students.

11. Engage effectively with appropriate external networks and external professional bodies.

Other duties

12. Stay abreast of regulatory changes including cybersecurity developments and their impact on IT requirements, including relevant data privacy requirements.

13. Continuously improve processes and implement tools for policy management

Person Specification

Information Security & Compliance Manager Grade: F

EDUCATION QUALIFICATIONS AND ACHIEVEMENTS:

Essential criteria

- Degree or equivalent qualification in Information Systems security or related technical discipline or relevant experience (A/I)

Desirable

- Certified Information Systems Security Professional (CISSP) (A/I)

KNOWLEDGE AND EXPERIENCE:

Essential criteria

- Proven experience in an information security role including experience of developing Information Security policies and plans (A/I)
- Working knowledge of the Data Protection Act (1998) and the incoming General Data Protection Regulations (GDPR)
- Excellent knowledge and understanding of information risk concepts and principles as a means of relating business needs to security protocols. (A/I)
- Excellent understanding of information security concepts, protocols, industry best practices and strategies. (A/I)
- Good understanding of system technology security testing (vulnerability scanning and penetration testing.) (I)
- Good understanding of higher education IT and information environment, preferably in security, compliance/audit or infrastructure. (I)

SKILLS AND ABILITIES:

Communication

- Excellent communicator able to reduce complex ideas to simple terms and express these both to non-technical and highly technical audiences (A/I)

Leadership

- Ability to drive consensus , influence and persuade others to take a specific course of action even when there is no direct line of command or control (A/I)

Liaison & networking

- Ability to work effectively and authoritatively with senior managers and colleagues across the University, (A/I)

Analysis & problem solving

- Experience of analysing complex issues, innovating to resolve problems and thinking strategically (A/I)

Service Delivery

- Demonstrable ability to work in a pressurised environment with conflicting priorities, ensuring that deadlines are met ensure high quality service (A/I)

Planning & Organisation

- Experience of planning, prioritising and organising the work of yourself and others, delivering to tight deadlines whilst ensuring the effective use of resources (A/I)

Other essential criteria:

Commitment to, and understanding of, equal opportunities issues within a diverse and multicultural environment. (I)