Job Description – Head of Cyber Operations and Incident Response

About the role

As a member of the Information Security team, you will ensure that the confidentiality, availability and integrity of the Open University’s information and information systems is protected. This will primarily be achieved through identification and recommendation of risk mitigation treatment plans and specialist security consultancy to support the needs of the university.

Key Responsibilities

- Support the Information Security leadership team with the implementation of the security strategy with regards to Cyber Operations and Cyber Incident Response.
- Design, build, implement, and refine Cyber Incident Response plans that consider the operational, tactical, and strategic elements of an effective Cyber Incident Response whilst considering existing Incident, and Crisis Response frameworks.
- Advise the organisations Business Continuity team and embed Information Security principles into the programme.
- Strategic reporting of Cyber Incidents through various governance boards.
- Manage security incidents using recognised industry standards/frameworks, such as MITRE ATTACK.
- Manage, and upskill a team of Cyber Analyst(s) who provide operational security expertise for the Information Security team.
- Ensure Cyber Operations, Cyber Incident Management, and Cyber aspects of Business Continuity are aligned to best practise.
- Develop, review, and embed Information Security Policy, associated standards, and guidance.
- Work closely with Information Rights (Data Protection) colleagues to embed breach management into Cyber Incident Response Plans.
- Support the auditing of Open University Information, and Information Systems.
- Maintain a working knowledge and track requirements of Law, Regulations, Standards and Frameworks as they pertain to Information Security.
- Leverage existing technologies and embed new technologies to bolster the organisations resiliency to Cyber Incidents.
- Provide technical expertise and support to Operational Security Analysts, or other colleagues within Security Operations, and Infrastructure Teams.
- Facilitate board, and operational level exercises to assess response plans and embed Cyber Incident Response procedures into the organisation.
- Upskill other Information Security Team members on effective Cyber Security Incident Response management.
- Translate Operational Cyber Security risk to the CISO, and board by aligning risks to the organisations published risk framework.
- Liaise with external bodies and organisations to keep abreast of emerging trends, technologies and legislation that have an impact on Information Security to maintain technical expert status.
Skills & Experience

- Demonstrable experience in leading within Security Operations and Incident Response
- Good interpersonal skills and the ability to deal with staff at all levels
- Excellent collaboration and team working skills
- Pro-active approach to the identification of incidents, problems, and improvement opportunities
- Commitment to ongoing personal development and refreshing expertise in response to technology change
- Ability to identify and adapt to change
- Ability to effectively prioritise, plan and organise tasks
- Proven ability to communicate effectively, orally and in writing, with people across a range of areas and levels
- Ability to support others to successfully adapt to change
- Capable of analysing data to evaluate risk and compliance
- Can build and develop effective relationships with internal and external stakeholders

Desirable: Degree in a security or technology related field and/or CBCI, CISMP, CISM, CISSP, GCIH