Post Title:	Operations Centre Manager
Grade:	8

Job Description

2.1. Purpose

The Operations Centre Manager will oversee the administration, support and operational security of products and services deployed on behalf of the University Group.

The post holder is charged with managing the detection of and response to operational and cybersecurity incidents and events. They will ensure that all aspects of the IT provision are monitored, vulnerability scans are performed, and events are analysed and assessed. Additionally, they will ensure that response plans are developed, maintained and enacted as appropriate.

The post will line manage and oversee the day to day working of the Operations Centre Team. They will ensure high team performance alongside developing a culture of learning and empowerment.

2.2. Main Duties and Responsibilities

1. Manages the Operations Centre Team. Allocates responsibilities and/or packages of work. Provides support and guidance as required, in line with individuals' abilities. Delegates responsibilities as appropriate. Advises individuals on career paths, and encourages pro-active development of skills and capabilities. Sets performance targets, and monitors progress against agreed quality and performance criteria. Provides effective feedback, throughout the performance management cycle, to ensure optimum performance.

2. Provides leadership associated with the planning, design and improvement of service and component availability. Includes the investigation of all breaches of availability targets and service non-availability, with the instigation of remedial activities. Plans arrangements for disaster recovery together with supporting processes and manages the testing of such plans.

3. Manages capacity modelling and forecasting activities. Pro-actively reviews information in conjunction with service level agreements to identify any capacity issues and specifies any

required changes. Provides advice to support the design of service components including designing in flexible and scalable capacity.

4. Responsible for collating and acting on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems.

5. Monitors the application and compliance of security administration procedures and reviews information systems for actual or potential breaches in security. Ensures that all identified breaches in security are promptly and thoroughly investigated and that any system changes required to maintain security are implemented. Contributes to the creation and maintenance of policy, standards, procedures and documentation for security.

6. Conducts investigations to correctly gather, analyse and present the totality of findings including digital evidence to both business and legal audiences. Collates conclusions and recommendations and presents forensics findings to stakeholders.

7. Coordinates and manages planning of penetration tests, within a defined area of business activity. Delivers objective insights into the existence of vulnerabilities, the effectiveness of defences and mitigating controls. Provides authoritative advice and guidance on the planning and execution of vulnerability tests. Defines and communicates the test strategy. Manages all test processes, and contributes to corporate security testing standards.

8. Provides technical expertise to enable the correct application of operational procedures. Uses infrastructure management tools to determine load and performance statistics. Identifies operational problems and contributes to their resolution. Provides reports and proposals for improvement, to specialists, users and managers.

9. Ensures that appropriate action is taken to anticipate, investigate and resolve problems in systems and services. Ensures that such problems are fully documented within the relevant reporting system(s). Enables development of problem solutions. Coordinates the implementation of agreed remedies and preventative measures. Analyses patterns and trends.

10. Ensures that incidents are handled according to agreed procedures. Investigates escalated incidents to responsible service owners and seeks resolution. Facilitates recovery, following resolution of incidents. Analyses causes of incidents, and informs service owners in order to minimise probability of recurrence, and contribute to service improvement.

11. Uses data centre management tools to produce management information on power, cooling and space and investigate issues where necessary. Carries out routine audit and checks to ensure adherence to policies and procedures. Facilitates the implementation of mandatory electrical safety testing.

12. Manages suppliers to meet key performance indicators and agreed targets. Manages implementation of supplier service improvement actions. Use suppliers' expertise to support and inform development roadmaps.

13. Manages aspects of the product lifecycle, working with colleagues in other disciplines to enable effective marketing and customer support. May act as product owner for one or more lower value products or services.

Deputises for the Head of Service Delivery as required.

AND such other duties as are within the scope of the spirit of the job purpose, the title of the post and its grading.

2.3. Supervision Received

Line management is from the Head of Service Delivery.

2.4. Supervision Given

Operations Centre Team.

2.5. Contacts

- IT Services staff, including Executive Team.
- University Group Leadership Team.
- Staff and students in other Schools / Support Areas of the University Group.
- External Suppliers and other education institutions.

3. Person Specification

ATTRIBUTES	ESSENTIAL	ADVANTAGEOUS
Education & Qualifications	• A degree relevant to IS/IT. • Or full membership of an IS/IT professional body. • Or substantial experience in lieu of the above which demonstrates a professional approach to IS/IT development.	• ITIL. • CISSP.
Knowledge & Experience	• Significant experience of leading a high performing team. • Significant experience of building and operating IT infrastructure. • Understanding global / local business differentiation. • Digital business literacy. • Tracking of emerging trends.	• Understanding of business organisation, politics and culture. • Ability to understand related industries. • Higher Education experience.
Interpersonal Skills	• Results and business orientated approach. • Able to work both collaboratively and within a team • Adaptable to task and approach • Openness to learning. • Communication, listening and information gathering. • Creative and innovative thinking.	• Conceptual thinking. • Strategic thinking. • Leading, inspiring and building trust.
Job-related Skills, Abilities & Competencies	• Supplier management. • Integrating solutions. • Understanding digital technologies. • Understanding existing systems and technology. • Problem solving. • Experience of operating a NOC and/or SOC. • Systems applications (authentication, email etc.) operational management. • Security applications (VMS, SIEM etc.) operational management. • Cyber-security. • Public cloud infrastructure. • Able to make decisions working	• Microsoft Azure. • Amazon Web Services.

	under pressure and to tight timescales. • Ability to influence and persuade peers and customers. • Confident working at all levels including executive level.	
Other Requirements	• A flexible approach to working hours and location, including a willingness to travel, locally, nationally or overseas, as required. • Requirement to work on call in order to facilitate the 24*7 support demands of a global organisation. • An appreciation of other cultures; the global reach of the University Group and its international agenda.	