Candidate Information

Position: Cyber Security Manager
School/Department: IT Systems and Services
Reference: 22/110428
Closing Date: Monday 5 December 2022
Salary: £43,414 - £53,353 per annum.
Anticipated Interview Date: Thursday 15 December 2022

JOB PURPOSE:

To lead the Cyber Security team in the developing, managing and implementing of strategies, policies, reports, and services to meet the University's cyber security needs.

MAJOR DUTIES:

1. Provide lead advice on all aspects of cyber security relevant to the protection of the University's cyber assets including assessments of cyber threats and of the effectiveness of the measures in place.
2. Implement and maintain the University Cyber Security Strategy on behalf of senior management.
3. Manage the cyber team, to implement the cyber security strategies and policies of the University. This includes recruitment, appraisal, staff development and resource management.
4. Take a lead role in the development and maintenance of tools and solutions to monitor and assess cyber security threats and to protect cyber assets from threats, working with other stakeholders across the University.
5. Take responsibility for preparing and presenting regular cyber security reports to senior management, both at project and executive level within the University.
6. Manage the University's Security Operations Centre (SOC); to ensure an effective response to cyber alerts and incidents.
7. Take a lead role in managing third party contractors e.g., Pen testers, Auditors etc.
8. Take responsibility for cyber awareness and maintain an effective cyber awareness program for the University.
9. Develop and maintain effective relationships with system owners, data owners and other key stakeholders, both inside and outside the University.
10. Provide high level specialist/professional advice to stakeholders. Develop appropriate training and documentation to support cyber security.
11. Lead and/or participate in teams and projects to improve cyber security across the University.
12. Develop, promote, and maintain appropriate policies and procedures to support cyber security.
13. Lead/participate in collaborative projects to provide services across different parts of the University.
14. Report to and participate in relevant committees and groups, both internal and external.
15. Contribute to the development and monitoring of divisional and team strategies and plans. Maintain an awareness of relevant University strategies and plans.
16. Keep up to date with issues, best practice and legislation relating to cyber security and ensure policies, services, etc. are responsive to current and emerging threats.
17. Ensure professional and quality standards are maintained and applied within the area of activity.
18. Carry out any other duties which are appropriate to the post as may be reasonably requested by senior management.

ESSENTIAL CRITERIA:

1. Relevant Degree or equivalent professional qualifications e.g. CISSP, CompTIA Security+ etc.
2. Substantial and proven knowledge and understanding of the security implications of infrastructure design, including:
   - Firewalls and intrusion detection technologies.
   - Strategies and techniques used by hackers, and the associated preventative measures.
   - Authentication, encryption, and user validation techniques e.g., Kerberos, Active Directory.

3. Proven experience of data capture and presentation tools e.g., Microsoft PowerBI and Power Automate.
4. Substantial breadth and depth of knowledge of security controls and procedures as applied to databases and operating systems including Linux and Windows.
5. Experience of creating and maintaining user support documentation, and self-help solutions with appropriate editorial style aligned to target audience.
6. Demonstrable and proven experience in development, implementation and monitoring of Information Security Policies and related policies and procedures.
7. Up-to-date knowledge of new techniques and practices and ability to advise regarding potential opportunities or benefits.
8. Good analytical skills, structured and methodical approach, highly organised.
9. Proven capacity for problem-solving and troubleshooting.
10. Ability to set clear objectives to teams and staff and ensure they have the appropriate responsibility and authority to achieve them.
11. Awareness of the degree of confidentiality regarding appropriate information.
12. Ability to perform and scope IT audits in line with best practice and to manage independent audits e.g., pen testing.
13. Conviction, drive, and ability to persuade and convince users to adopt new ways of working.
14. Demonstrable ability to produce high level reports.
15. Excellent communication skills, both oral and written.
16. Demonstrable ability to communicate technical information to colleagues and non-technical users of all grades with clarity and effectiveness.
17. Ability to act as a leader, inspire confidence and assist others to adapt to change.
18. Ability to work autonomously with minimal management supervision, exercising judgement on when to refer issues to higher management.
19. Excellent interpersonal and organisational skills.
20. Keen to learn and undertake suitable training in relevant technologies.
21. Must be willing to provide cover, as required, during weekends and evenings, over critical periods and over some holiday periods as required in accordance with the needs of the Service.

DESIRABLE CRITERIA:

1. BCS Professional / Chartered Membership or equivalent.
2. Hold or be in the process of obtaining a Cyber Security Professional qualification e.g., CISSP, CompTIA Security+ etc.
3. ITIL certification foundation level or greater.
4. Proficient in and experienced in general project management concepts e.g., Agile, PRINCE II etc.
5. Experience in the implementation of ISO 27001.
6. Experience of using IT Security audit tools e.g., Nessus Pro, Tenable SC.
7. Experience of direct management of professional IT staff including responsibilities such as: appraisal of staff; staff development; resource/project management.
8. Sound understanding of budgetary and financial information, with demonstrable ability to produce costed proposals and business cases.
9. Commitment to Quality Standards and continuous improvement.
10. Interests /activities that develop leadership /teamwork skills.