Job Description

Head of Cyber Security

Salary:	Grade 9
Contract:	Full time, ongoing
Location:	Canterbury Campus
Responsible to:	Deputy Director of Information Services
Responsible for:	Cyber Security Team
Job family:	Administrative, professional and managerial

Job purpose

The Head of Cyber Security will provide strategic leadership in the development and implementation of cybersecurity policies, procedures, and best practices in alignment with industry standards and regulations.

Leading our cyber security strategy and delivery, this role demands a highly skilled technical expert who can lead from the front, and is very much hands-on, ensuring the security and integrity of the university's digital assets.

The ideal candidate will possess a strong technical background, proven leadership capabilities, and the strategic vision to advance our cyber security posture. You will have a passion for Cyber Security, deep understanding of the industry and willingness to bring new ideas and challenge the status quo.

Key accountabilities

The following are the main duties for the job. Other duties, commensurate with the grading of the job, may also be assigned from time to time.

- Lead on the creation and implementation of the University’s Cyber Security strategy, advocating the importance of cyber security investment and prioritisation to senior leaders including IT SMT, executive and council.
- Provide assurance, specialist guidance and reporting on the effectiveness of the Cyber Security strategy and posture to senior leaders of the University including Information Services SLT, executive group and council.
- Work in partnership with external service providers to provide specialist services in order to enhance organisational capability and capacity. Oversee performance, ensuring that Service Level Agreements (SLAs) are met or exceeded, and any issues or disputes are resolved quickly.
- Develop and oversee incident response plans, ensuring rapid and effective response to cybersecurity incidents, and conducting post-incident analysis to improve security measures.
- Identify and assess cybersecurity risks and vulnerabilities, and develop and implement risk mitigation strategies to protect the university's assets.
- Promote cybersecurity awareness and best practices among staff and students through training and awareness campaigns.
- Maintain a strong technical understanding of current and emerging cybersecurity threats, technologies and trends, and provide technical guidance and support to the team and specialist IT sections within the department.
- Ensure compliance with relevant cybersecurity regulations, conduct regular security audits, and liaise with external auditors as needed. Oversee the continuous improvement roadmap, implementing security accreditation and assessment frameworks e.g. ISO 27001, Cyber Essentials Plus, CAF etc
- Evaluate, recommend, and implement cybersecurity tools and technologies in partnership with teams across IS to enhance the university's security posture.

- Manage the University's Cyber Security budget, allocating and planning spend, ensuring Cyber Security is appropriately resourced and operating effectively and efficiently. Develop comprehensive business cases for enhanced cyber security services and make the case for associated investment at senior levels.
- Ensure the effective monitoring of network traffic and systems for signs of suspicious or malicious activity and respond appropriately to detected threats.
- Represent Information Services in Cyber security at all levels, championing the importance of cyber security and influencing decision making.

Key challenges and decisions

The following provide an overview of the most challenging or complex parts of the role and the degree of autonomy that exists.

- Provide strategic leadership in cyber security, developing and delivering a cyber security strategy and roadmap. Translating complex technical challenges into clear, actionable insights for senior leaders including the IS SMT, executive group and council.
- Ensuring robust security measures while maintaining accessibility for students and staff to the necessary resources.
- Building and maintaining strong relationships with service providers and university stakeholders. Using effective communication, negotiation, and conflict resolution ensure improve the university's cybersecurity stance while meeting stakeholder needs.

Facts & figures

Budget: Cyber Security budgets from multiple sources estimated to be over £500,000 per annum
Hardware: ~650 VM's, ~750TB Data, ~200 physical servers, ~6000 endpoint devices, ~1000 network switches, ~2900 Wi-Fi access points
Cyber Team: 4 people

Internal & external relationships

- **Internal:** Colleagues within Information Services, Academic and Professional Services Managers and staff, students, Senior Leadership Team (SLT), Executive Group (EG), Council

- **External:** Managed service provider(s), technology vendors/suppliers, consultants, partners and stakeholders, professional bodies and networks

Health, safety & wellbeing considerations

This job involves undertaking duties which include the following health, safety and wellbeing considerations:

- Regular use of Screen Display Equipment
- Pressure to meet important deadlines such as might be inherent in high profile projects
- Ability to travel in a timely and efficient manner regularly between campuses

Person specification

The person specification details the necessary skills, qualifications, experience or other attributes needed to carry out the job. Applications will be measured against the criteria published below.

Selection panels will be looking for clear evidence and examples in an application, or cover letter (where applicable), which back-up any assertions made in relation to each criterion.

Essential Criteria:

- Bachelor's degree in Computer Science, Information Security, or a related field or equivalent experience (A)
- Significant experience in a hands-on cybersecurity role(s) with a strong technical background (A,I)
- Experience leading the design and implementation of cyber security strategies and policies (A,I)
- Strong technical skills in cyber security, including: Network security, System security, Application Security, Incident response (A,I)
- Systems Administrator experience with Windows or Linux (A,I)
- Proven track record of successful team leadership and management (A,I)
- In-depth knowledge of cybersecurity frameworks, standards, and best practices, with a strong ability to translate technical concepts for non-technical stakeholders (I)
- Ability to effectively manage relationships with vendors and external manage service providers, including negotiating contracts, defining SLAs, and ensuring compliance with contractual obligations (I)
- Experience with IT technical evaluation, procurement and implementation (I)
- Experience implementing industry best practices frameworks and securing cyber accreditation. e.g. cyber essentials, ISO27001 (I)
- Experience of budget management and financial planning (I)
- Strong analytical and problem-solving skills, with the ability to assess and mitigate complex cybersecurity risks and vulnerabilities (I)
- Proven experience in conducting audits, ensuring compliance with relevant regulations, and liaising with external auditors (I)
- Able to advocate and influence cyber security across team, department, university and with external partners (I)
- Experience leading a customer centric approach to service delivery and change management, having led large, organisational wide change projects (I)
- Firm commitment to achieving the University’s vision and values, with a passion for a transformative student experience and multidisciplinary, impactful research (I)
- Commitment to deliver and promote equality, diversity and inclusivity in the day to day work of the role (I)

Desirable Criteria:

- Member of a professional body in a relevant discipline (A)
- Professional certifications such as CISSP, CISM, CISA or equivalent (A)

Assessment stage: A - Application; I - Interview; T - Test/presentation at interview stage