Job description: Chief Information Security Officer

REPORTING TO: Chief Information Officer

LOCATION: Milton Keynes

We believe that where you start in life, shouldn’t limit where you go.

Our search is now on for an exceptional Chief Information Security Officer who is a Cyber Security leader. They will devise and implement the information security strategy and policies that will protect The Open University’s assets, 8,000 staff and 174,000 students.

The Open University is a unique institution created 50 years ago to open up education for all. We are open to anyone, anywhere, changing millions of lives across the world and always looking for new ways to help people succeed. Our pioneering use of innovative methods, such as our BBC partnership, means we reach more people than any other University.

We work across all four nations of the UK and we are the most popular choice for online, distance, flexible study.

CIO Portfolio

The CIO Portfolio brings together areas of the University to improve the provision of service, assurance and governance across Technology, Data, Change, Information Security, plus programmes and projects including the Core Systems Replacement Programme, which is one of the strategic priorities of The Open University. It is a highly skilled, joined-up team, focused on bringing their resources together to serve the University and better support the students.

About the role

The Chief Information Security Officer is an Executive role within the CIO Portfolio which services the entire University. The role holder will provide a clear vision and direction for information and Cyber Security operations. They will promote continuous improvement, innovation and agility in service delivery, whilst working in consultation and collaboration with colleagues across the University.

As the Chief Information Security Officer, you will be responsible for overseeing a range of technical and process security controls and leading a programme of continuous improvement in response to changing security threats and risk.

The role requires a thorough understanding of the technology underpinning the University’s IT systems, as well as a broad, up-to-date knowledge of information security frameworks, pertinent regulation and legislation, vulnerability management, incident management and response, secure development techniques and approaches, Cyber Security engineering and operations, and management and governance of Cyber risk and Cyber Security.

Having performed a similar role in a large, distributed organisation, you will have a strong information and Cyber Security background along with formal qualifications. You will have established and led a large, progressive information security function, developing innovative, future focused information and Cyber Security capability in support of business objectives. You will be a
This is a fantastic opportunity to join a world class institution in a pivotal and highly visible leadership role which will require high levels of personal energy and commitment.

Key responsibilities

Information and Cyber Security Strategic Direction

- Define, develop and maintain a business-aligned Information and Cyber Security strategy and operating model
- Define and embed an Information Security Policy Framework across the University that addresses the needs of the University, its staff, students, and other external stakeholders in line with relevant legislation and industry standards
- Provide advice and direction to the University’s senior leadership team (Vice Chancellor’s Executive), in the integration of security practices into the University’s strategic and operational processes
- Drive and deliver change to the University’s Information and Cyber Security systems, processes and procedures by continuously analysing and reviewing new security technologies and practices as informed by industry best practice
- Report to university committees and management groups on Information and Cyber Security matters
- Represent the University on national and international external consortium groups and boards and engage effectively in appropriate external networks, ensuring the Open University can anticipate, meet and respond to new Information and Cyber Security challenges and threats

Leadership and People Management

- Develop and lead an effective, high-performance Information Security team retaining and attracting key talent to ensure continuous improvement in staff competencies, skills and knowledge
- Establish and maintain clear and measurable Information and Cyber Security strategic plans, budgets and targets, and robust and fit-for-purpose operational procedures and deliver measurable service improvements and ensure that all elements of the service represent the best value for money
- Ensure that the culture, policies, structures and reporting systems are in place to allow the Information Security team to achieve the highest standards of quality, legal and regulatory compliance and corporate governance in all areas
- Play an effective role as a member of the CIO Portfolio Executive in the leadership of the Unit
- Foster a culture of innovation and continuous improvement that encourages, engages and supports a high level of professional development and personal responsibility
- Ensure that the Unit’s resources and budget are managed effectively, in accordance with institutional policy and procedures, and provide best value for money to the University’s students and staff
- Provide the Information Security team with high-quality and empowering leadership, setting and delivering the highest service standards and a strong performance culture by developing and sustaining best practice within the Unit
Information and Cyber Security Management

• Provide senior leadership and oversight of effective information and Cyber Security risk management, integrated with the University’s institutional risk management framework
• Ensure that information and Cyber Security risks to the University presented through suppliers and delivery partners are identified and managed appropriately
• Develop and maintain an effective Information Security Management System and processes for continual improvement
• Ensure Information Security is managed effectively throughout the IT service delivery lifecycle (incl. Security Operations, Security Architecture and Security Assurance)
• Lead on development and delivery of measures and metrics to support the assessment, reporting and ongoing improvement of the information security posture
• Work closely with internal stakeholders and business units to keep abreast of planned changes to technologies, working practices, and business activities that could have an impact on the University’s Information Security or risk profile
• Define and implement an appropriate information assurance framework for the University, enforcing compliance with policies in conjunction with internal audit
• Ensure and promote an appropriate level of information security culture and awareness across the University
• Direct, and assist as necessary, investigations into information security breaches and pursue associated disciplinary and legal matters, liaising with the Information Rights team on data protection legislation ensuring root-causes of such breaches are understood and addressed

Person specification

EXPERIENCE

• Substantial experience in senior management in a complex IT organisation encompassing service delivery, application development and IT infrastructure
• A track record in the management and delivery of transformational security improvements across an organisation
• Proven experience at engaging, influencing and managing stakeholders across departmental and organisational boundaries up to and including director/Vice Chancellor Executive level
• A track record in directing and managing innovative change and continuous improvement, ensuring excellent organisational performance and outcomes across a complex portfolio of responsibilities
• Proven experience at managing complex budgets and resources with a track record of identifying and securing approval for business cases at enterprise level for organisational investment in information and cyber security
• Experienced in leading, developing and motivating a team of subject matter experts

KNOWLEDGE

• An excellent understanding of best practice within Information Security and risk management including standards such as ISO/IEC 27001, Cyber Essentials and CObIT
• An excellent understanding of legislation and regulations that impact information Security E.g. Data Protection Act (2018), Freedom of Information Act, PCIDSS
• An understanding of current and emerging threats and countermeasures and the organisational challenges to addressing these threats
• An understanding of Application Security threats and countermeasures
A good practical knowledge of security technologies and wider business solutions including Firewalls, IDS/IPS, Identity and access management, SIEM, remote working and cloud technologies

SKILLS

- A collaborative leader with strategic acumen and problem-solving skills, able to inspire and motivate colleagues
- An ability to articulate strategy in an empowering, collegiate and inspiring way which also informs transparent, viable and sustainable planning processes
- The ability to work within a regulatory framework and to articulate its potential as a tool for continuous improvement
- Demonstrable creativity and a commitment to future-proofing service and delivery in a fast paced, ever-changing environment
- A Self Starter with the ability to lead and drive change through an organisation
- Excellent communication skills, both written and verbal. Ability to present complex or highly technical issues in simple and easy-to-understand formats
- Ability to build strong relationships and influence decisions with internal and external stakeholders
- A good understanding of project management methodology and how to implement security within them
- Good analytical skills and the ability to challenge the norm
- An ability to think and plan strategically and systematically while recognising the need to deliver to the business requirements
- The ability to be pragmatic while balancing the needs of the University against security
- The ability to cut through organisational and political barriers to achieve the overall goal

Qualifications

- An appropriate degree, equivalent qualification or experience
- One or more of the following qualifications are highly desirable:
  - Certified Information Security Manager (CISM)
  - Certified Information Systems Security Professional (CISSP)
  - Certified Information systems Auditor (CISA)
  - MSc Information Security
  - Achieved Senior or Lead level certification in the NCSC’s Certified Cyber Professional scheme in one or more of Security and Information Risk Advisor (SIRA), IA Architect, IA Auditor, IT Security Officer
  - Full membership of the Institute of Information Security Professionals
  - Prince 2/PMP

AREAS WHICH FORM THE CIO PORTFOLIO

- Learning Experience and Technology
- Data and Student Analytics
- Strategic Technology Programmes
- Information Technology
- Change and Improvement
- Information Security