Job Description

Job title:	**Chief Information Security Officer (CISO)**
Department/School:	**Digital Data & Technology**
Grade:	**ALC6**
Location:	**University of Bath**
Position Number:	**CY101**
Last reviewed:	**July 2023**

Job purpose

The Chief Information Security Officer (CISO) is accountable for all information and cyber security across the University of Bath (UoB). They are responsible for safeguarding the information assets and delivering the Cyber Security Strategy. The CISO maintains and improves security posture via a risk-based approach that complies with industry standards and the UoB's risk and controls frameworks.

Leading all information security activities, the CISO manages information and technology risk, responds to both internal and external threats and advises the University at a strategic level on the changing threat landscape. The role owns and develops appropriate security policy, standards, and procedures to protect the University's assets, staff and students.

Responsibilities:

- **Information Security Strategy**: Develop and execute a clear vision and robust information security strategy aligned with the UoB's overall goals and objectives. Identify potential risks, vulnerabilities and threats implementing proactive measures to mitigate them effectively.
- **Compliance and Risk Management**: Ensure compliance with relevant regulatory requirements, industry standards and best practices. Establish and maintain a comprehensive risk management framework to identify, assess and mitigate potential security risks.
- **Policy and Procedure Development**: Establish and enforce information security policies, procedures and guidelines that align with industry best practices, statutory and regulatory requirements. Regularly review and update these policies to reflect changes in technology, regulations and emerging threats.
- **Security Architecture:** Design, implement and maintain a secure and resilient information technology infrastructure ensuing confidentiality, integrity and availability of systems, networks and data through effective security controls.
- **Incident Response and Recovery**: Develop and implement an Incident Response Plan to promptly address and mitigate security incidents, breaches, and other cyber threats. Coordinate with internal stakeholders and external vendors to resolve issues and restore normal operations in a timely manner.
- **Security Awareness and Training**: Promote a strong security culture throughout the organisation by implementing security awareness programmes, training sessions and workshops. Educate employees on information security best practices, policies and their role in maintaining a secure environment.
- **Vendor Management**: Evaluate, select and manage third-party vendors and service providers to ensure their compliance with security standards and protect the organisation's interests. Conduct regular assessments of vendor security controls and address any identified vulnerabilities or weaknesses.
- **Security Incident Monitoring and Reporting**: Establish robust security monitoring capabilities to detect and respond to potential threats. Generate regular reports and metrics on security

incidents, risks, and trends to keep stakeholders informed about the organisation's security posture.

Source and nature of management provided
Chief Information & Digital Officer (CIDO)

Staff management responsibility
Direct and line manage the core Cyber team plus provide advice, guidance motivation and direction to the DTP community. Line management of a multi – skilled technical team of staff. The post holder will be expected to adhere to UoB HR Policies and Guidelines.

Special conditions
You will from time to time be required to undertake other duties of a similar nature as reasonably required by your line manager. This will form part of your substantive role and you will not receive additional payment for these activities. The University operates an "out-of-hours" system to ensure service continuity. The post-holder will be required to join the out-of-hours list and undertake occasional duties outside of standard University hours including evenings or weekends. Annual leave may be restricted during peak workload periods. The post-holder will ensure full compliance with all Data Protection laws and UoB policies and guidelines.

Main duties and responsibilities	
1	**Information and Cyber Security Strategic Direction** • Define, develop, and maintain a business-aligned Information and Cyber Security strategy and operating model in consultation with the relevant stakeholders. • Define and embed a UoB Information Security Policy Framework that addresses the needs of the University, its staff, students and 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) on all operational and strategic matters relating to information & Cyber Security. • Provide thought leadership to cyber initiatives across the UoB. • 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 University can anticipate, meet, and respond to new Information and Cyber Security challenges and threats.

2	**Information and Cyber Security Management** • Provide senior leadership and oversight of effective information and Cyber Security risk management, integrated with the University's corporate 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. • Oversee an organisation wide education and awareness programme, driving understanding, engagement and support on cyber risks and topics across the entire university. • Direct, and assist as necessary, investigations into security incidents and data breaches and pursue associated disciplinary and legal matters. Liaise with the appropriate departments on data protection legislation ensuring root-causes of such breaches are understood and addressed. • Represent the University on national and international external consortium groups and networks including JANET CSIRT, UK Security, CISP, CESG • Develop links with security experts in HE and beyond, ensuring UoB is aware of, and can respond to, emerging Information and Cyber Security challenges.
3	**Leadership and People Management** • Provide high-quality and empowering leadership delivering the highest service standards and a strong performance culture by developing and sustaining best practice. • Develop and lead an effective, high-performance Cyber Security team. Attract and develop staff to ensure continuous improvement in staff competency, skills and knowledge. • Establish and maintain clear, measurable service improvements and ensure all elements of the service represent the best value for money. • Ensure effective culture, policies, structures and reporting systems so the Cyber Security team can achieve the highest standards of quality, legal and regulatory compliance, and corporate governance. • As a proactive, supportive member of the DDaT Senior Leadership Team inform the strategic and operational planning and delivery of departmental activity and outputs. • Drive a culture of innovation and continuous improvement that encourages and supports a high level of professional development and personal responsibility.
4	**Financial management** • Lead the financial management of the Cyber activity ensuring production and distribution of financial management information to relevant staff and Boards. • Participate in the annual budget planning process/create business cases to secure budget/funding for information & cyber security operations and projects. • Ensure that resources and budget are managed effectively, in accordance with policy and procedures to provide best value for money to the University. • Provide support for the financial processing of expenditure as required.
5	**General** • Member DDaT Senior Leadership Team.

	• Attend /advise/ Chair UoB meetings as directed by CIDO. • Communicate and build strong, positive working relationships with staff at all levels including UoB Executive Board members. • Resolve issues on own initiative and judgement, liaising with other stakeholders as necessary. • You are required to always follow University policies and procedures and take account of UoB guidance. • Undertake any other activities assigned from time to time by the CIDO. • Occasional travel may be required, for example to user groups or conferences. • In undertaking these responsibilities, the post holder can delegate responsibility, but not accountability, for specific functions to other individuals.
Commitment to the University's Effective Behaviours Framework As a holder of the Association of University Administrators Mark of Excellence Award, the University has identified a set of effective behaviours which we value and have found to be consistent with high performance across the organisation. Professional Services staff are expected to exhibit these behaviours with a commitment to on-going personal development in these areas. Further details are outlined in the person specification.	

Person Specification

Criteria: Qualifications and Training	Essential	Desirable
Educated to higher degree level in an appropriate subject or equivalent experience in a related field	X	
ILM (Level 3) Qualification or equivalent leadership and management experience	X	
Qualification in Information Security, such as Certified Information Systems Security Professional (CISSP), CISA or similar, or have equivalent experience in the field	X	
Professional project management qualification (e.g., PRINCE2 foundation or equivalent)		X
ITIL (Version 3 or later) Foundation Level Qualification [or with training have achieved this qualification within their probation period]	X	

Knowledge and experience	Essential	Desirable
Significant experience in senior management in a complex IT organisation encompassing service delivery, application development and IT infrastructure	X	
Expert knowledge of best practice within Information Security and risk management including ISO/IEC 27001, Cyber Essentials and CObIT	X	
Good practical knowledge of security technologies and wider business solutions including Firewalls, IDS/IPS, Identity and access management, SIEM, remote working and cloud technologies	X	
Excellent awareness of current and emerging threats and countermeasures and the organisational challenges to addressing these threats	X	
Expert knowledge of Application Security threats and countermeasures	X	
Deep understanding of legislation and regulations that impact information Security e.g., Data Protection Act (2018), Freedom of Information Act, PCIDSS	X	
Successful management and delivery of transformational security improvements across an organisation	X	
Experience of engaging, influencing, and managing stakeholders across departmental and organisational boundaries including Board level	X	
Experience of directing and managing innovative change and continuous improvement, ensuring excellent organisational performance and outcomes across a complex portfolio of responsibilities		X
Proven ability to manage complex budgets and resources including producing and securing approval for business cases at enterprise level for organisational investment in information and cyber security.		X
Experienced in leading, developing and motivating a team of subject matter experts	X	

Skills and aptitudes	Essential	Desirable
Collaborative leader with strategic acumen and problem-solving skills, able to inspire and motivate colleagues	X	
Able to articulate strategy in an empowering, collegiate and inspiring way which also informs transparent, viable and sustainable planning processes	X	
Able to work within a regulatory framework and articulate its potential as a tool for continuous improvement	X	
Demonstrable creativity and commitment to future-proofing service and delivery in a fast paced, ever-changing environment	X	
Highly self-motivated with the ability to lead and drive change	X	
Excellent communication skills, both written and verbal. Able to present complex or highly technical issues in simple, easy-to-understand formats.	X	
Able to build strong relationships and influence decisions with internal and external stakeholders	X	

Application of project management methodology and how to implement security within them	X	
Good analytical skills and the ability to challenge the norm	X	
Able to think and plan strategically and systematically while recognising the need to deliver to the business requirements	X	
Pragmatic while balancing the needs of the University against security	X	
Excellent organisational skills, able to achieve results for multiple, simultaneous projects with competing demands	X	
Diplomacy to cut through organisational and political barriers to achieve the overall goal	X	
Calm and effective under pressure (e.g., when coordinating emergency incident responses)	X	
Able to deal with confidential and sensitive information with tact and discretion.	X	

Effective Behaviours

The University has identified a set of effective behaviours consistent with high performance across the organisation. They do not examine technical competence, rather they identify the behaviour patterns that are valued due to them being consistent with high performance across the organisation. This table below identifies how the EBF applies to this specific role. Part of the selection process for this post will be to assess whether candidates have demonstrably exhibited these behaviours previously.

Managing self and personal skills:

- Willing and able to assess and apply own skills, abilities, and experience.
- Being aware of own behaviour and how it impacts on others.

Delivering excellent service:

- Providing the best quality service to all students and staff and to external customers e.g., clients, suppliers.
- Building genuine and open long-term relationships in order to drive up service standards.

Finding innovative solutions:

- Taking a holistic view and working enthusiastically and with creativity to analyse problems and develop innovative and workable solutions.
- Identifying opportunities for innovation.

Embracing change:

- Adjusting to unfamiliar situations, demands and changing roles.
- Seeing change as an opportunity and being receptive to new ideas.

Using resources:

- Making effective use of available resources including people, information, networks, and budgets.
- Being aware of the financial and commercial aspects of the University.

Engaging with the big picture:

- Seeing the work that you do in the context of the bigger picture e.g., in the context of what the University/other departments are striving to achieve and taking a long-term view.
- Communicating vision clearly and enthusiastically to inspire and motivate others.

Developing self and others:

- Showing commitment to own development and supporting and encouraging others to develop their knowledge, skills, and behaviours to enable them to reach their full potential for the wider benefit of the University.

Working with people:

- Working co-operatively with others in order to achieve objectives.
- Demonstrating a commitment to diversity and applying a wider range of interpersonal skills.

Achieving results:

- Planning and organising workloads to ensure that deadlines are met within resource constraints.
- Consistently meeting objectives and success criteria.