CHIEF INFORMATION SECURITY OFFICER (CISO)

DEPARTMENT/UNIT	Office of the CIO
FACULTY/DIVISION	Information Technology Security and Risk
CLASSIFICATION	Executive
WORK LOCATION	738 Blackburn Road, Notting Hill

ORGANISATIONAL CONTEXT

Monash is a university of transformation, progress and optimism. Our people are our most valued asset, with our academics among the best in the world and our professional staff revolutionising the way we operate as an organisation. For more information about our University and our exciting future, please visit www.monash.edu.

eSolutions leads and directs the provision of IT solutions to the University. eSolutions is currently leading substantial technological, service and organisational reform towards creating a single IT function for the University that operates according to the following vision:

We partner with our customers to provide complete solutions enabling the Monash academic mission and delivery of the strategic agenda. We aim to be a customer focused organisation delivering flexible, responsive, coherent ICT services.

POSITION PURPOSE

The Chief Information Security Officer (CISO) reports to the Chief Information Officer (CIO) and is responsible for the development and delivery of the University's information security strategy and practice and leads and directs the IT Security & Risk team. This includes leading, coordinating, directing and reviewing the university-wide strategic and operational activities in the digital and IT security and risk area. This includes projects, strategic direction and planning, reporting, business improvement, performance measurement, and budget.

This position requires an experienced, energetic, engaging and visionary leader to lead an exciting, vibrant community of information technology professionals in protecting Monash and its array of digital assets. This in turn allowing Monash University to succeed in its mission to provide international excellence in both research and education.

Digital and information technology plays a vital and ever-expanding role in the University's mission. The information technology environment is complex - highly distributed and diverse. The University's Chief Information Security Officer (CISO) is therefore critical to ensure the design and implementation of a university-wide vision & strategy resulting in appropriate action planning that will ensure Monash University's Information Security governance both now and into the future.

The CISO is a member of the CIO leadership team and serves a key role in University leadership, engaging and working closely with senior internal and external stakeholders on complex and sensitive issues. The CISO engages and advises a range of senior stakeholders including senior Monash administration, academic leaders, General Counsel, Privacy, Enterprise Risk and Compliance and Internal Audit.

The CISO is an advocate for the University's total digital and information security needs and is responsible for the development and delivery of a comprehensive information security strategy to optimise the security posture of the University. The CISO leads the development and implementation of a security program that leverages collaborations and campus-wide resources, facilitates information security governance, advises senior leadership on security direction and resource investments, and designs appropriate policies to manage information security risk. The complexity of this position requires a leadership approach that is engaging, imaginative, and collaborative, with a proven ability to work with other senior leaders to ensure the optimal balance between security considerations and organisational priorities.

Reporting Line: The position reports to CIO

Supervisory Responsibilities: This position provides direct supervision to 4 direct reports, 14 indirect and management of various third parties

Financial Delegation: Yes, in accordance with the University delegations schedule

Budgetary Responsibilities: Yes, in line with Key Responsibilities

KEY RESPONSIBILITIES

Information Security Governance

1. Provide leadership in design of best practice methodology of Information Security organisational policies, procedures and processes in line with relevant legislation and industry standards
2. Provide leadership direction and support to Senior Monash leaders in the integration of security practices into the University's strategic and operational planning processes
3. Lead major projects and change initiatives driven by the Information Security strategy including Security Assurance Programs and Security Control Review based on the current and future threat landscape
4. Attend and report to the relevant Monash University steering committees and advisory boards on information security related matters
5. Preparation and presentation of regular reports for consideration by Senior Monash stakeholders across all Faculties and Divisions
6. Exercise strong budget management for the project(s) managed to a value of $8 million

Information Security Management

7. Lead & sponsor the establishment of forums and other communication and consultation channels that will result in an uplift in security practices and capabilities at the University
8. Engage with architecture and delivery teams to ensure projects and applications are designed and implemented in line with organisational information security policy and industry best practice
9. Direct and manage the monitoring of new and ever evolving threats and engage with internal and external stakeholders to ensure appropriate and on-going security controls are in place
10. Work with internal and outsourced IT teams to ensure the suitability of controls implementation and assurance over the implementation of those controls on an ongoing basis

Organisational IT Risk Management

11. Provide senior leadership and oversight of Monash University's IT risk posture and articulate emerging trends

12. Formally assess the organisational risk appetite of Monash Senior leaders and subsequently design, plan and manage Information Security governance strategies & plans aligning to organisational goals
13. Lead the continuous improvement review and analysis of new security technologies and practices as informed by industry best practice inside and outside of Higher Education and Monash experience to date
14. Orchestrate the development and implementation of key policies, processes and tools that are integral to monitoring, tracking, analysing and reporting on security risk across the organisation

Management

15. Exercise strong financial management and ultimate accountability for delivering within operational budget targets
16. Provide leadership, direction, support and mentoring to the IT Security & Risk team with specific attention to retaining and attracting key talent to ensure continuous skill and knowledge uplift
17. Build & sustain mutually beneficial networks and relationships, consult with industry experts and ensure up-to-date knowledge of emerging industry trends

KEY SELECTION CRITERIA

Education/Qualifications

1. The appointee will have:
    - Extensive experience in similar role;
    - a relevant postgraduate qualification and extensive experience at a senior level in Information Security, or an equivalent combination of extensive relevant senior level experience in Information Security and relevant education/training;
    - proven extensive knowledge of Risk and Security Frameworks i.e. ISO27001, ISO27002, ISO 31000;
    - industry certifications such as Certified Information Systems Security Professional (CISSP) or Certified Information Security Manager (CISM) are desirable

Knowledge and Skills

2. Exceptional leadership skills with proven ability to strategically manage and provide authoritative technical and policy advice at the highest levels
3. Exceptional strategic planning skills with the ability to create and implement a vision in line with Organisational goals & identified Information Security priorities and challenges
4. Outstanding organisational skills, with experience in establishing priorities, allocating resources and meeting deadlines whilst working with Senior stakeholders in a large, complex organisation
5. Extensive staff management experience with the ability to inspire, motivate and develop high performance teams
6. Exceptional analytical and conceptual skills including demonstrated ability to quickly assimilate new concepts and information and deliver positive, innovative solutions in line with required organisational goals and industry standards
7. Outstanding interpersonal and written and verbal communication skills with the ability to negotiate, influence and build consensus at senior levels and with diverse stakeholders on complex, highly technical issues
8. Extensive knowledge of national and international regulatory compliance and frameworks
9. Demonstrated expertise in financial management

OTHER JOB RELATED INFORMATION

- Travel to other campuses of the University may be required
- There may be a requirement to work additional hours from time to time
- There may be peak periods of work during which taking of leave may be restricted
- The incumbent is required to hold a Police Check

LEGAL COMPLIANCE

Ensure you are aware of and adhere to legislation and University policy relevant to the duties undertaken, including: Equal Employment Opportunity, supporting equity and fairness; Occupational Health and Safety, supporting a safe workplace; Conflict of Interest (including Conflict of Interest in Research); Paid Outside Work; Privacy; Research Conduct; and Staff/Student Relationships.