Position Description

Director, Cyber Security (Chief Information Security Officer (CISO))

Position Number: XXXXXX *Position Title: Director, Cyber Security (Chief Information Security Officer (CISO))* *Date Written: January 2020*	*Faculty / Division: Finance & Operations* *School / Unit: UNSW IT* *Position Level: Senior Appointment*

ORGANISATIONAL ENVIRONMENT

UNSW is currently implementing a ten year strategy to 2025 and our ambition for the next decade is nothing less than to establish UNSW as Australia's global university. We aspire to this in the belief that a great university, which is a global leader in discovery, innovation, impact, education and thought leadership, can make an enormous difference to the lives of people in Australia and around the world.

Following extensive consultation in 2015, we identified three strategic priority areas. Firstly, a drive for academic excellence in research and education. Universities are often classified as 'research intensive' or 'teaching intensive'. UNSW is proud to be an exemplar of both. We are amongst a limited group of universities worldwide capable of delivering research excellence alongside the highest quality education on a large scale. Secondly, a passion for social engagement, which improves lives through advancing equality, diversity, open debate and economic progress. Thirdly, a commitment to achieving global impact through sharing our capability in research and education in the highest quality partnerships with institutions in both developed and emerging societies. We regard the interplay of academic excellence, social engagement and global impact as the hallmarks of a great forward-looking 21st century university.

To achieve this ambition we are attracting the very best academic and professional staff to play leadership roles in our organisation.

Values in Action: Our UNSW Behaviours

UNSW recognises the role of employees in driving a high performance culture. The behavioural expectations for UNSW are below.

OVERVIEW OF RELEVANT AREA AND POSITION SUMMARY

UNSW IT is part of UNSW's Finance and Operations Division and provides high quality, sustainable, flexible products and state of the art services to UNSW. Our priorities are to drive innovative architectures that enable UNSW's digital future and to be a trusted partner of the University.

In recent years UNSW IT has implemented a Shared Service capability moving away from a complete federated model of individual IT units operating within Faculties and Divisions. UNSW IT is now entering its next phase of transformation to position itself as a strategic partner and enabler within the University.

A key and strategic role to UNSW, the position of Director, Cyber Security (Chief Information Security Officer (CISO)) is a high-visibility and critical leadership role. The role has clearly established autonomy, authority, and accountability for actions and decisions related to UNSW cyber security and Cyber risk; including consideration for information technology, financial, reputation, and people. The role also heads the enterprise identity and identity management function within UNSW and therefore has responsibility to ensure a well-designed and well-managed identity function and teams.

The role has visibility, exposure, and access to some of the most sensitive and critical data, information, materials, and assets of UNSW and therefore the CISO must be discrete and completely trustworthy.

The role of Director, Cyber Security (Chief Information Security Officer (CISO)) reports to the Chief Digital Officer. The CISO is expected to contribute to and support the broader UNSW IT function. The CISO has 3 direct reports. Within a team of 15 permanent employees. There are also variable contractor resources, based on the changing needs of the University.

RESPONSIBILITIES

Specific responsibilities for this role include:

- Provide strategic cyber thought leadership to the University senior management and Council to enable informed decision making.
- Maintaining the Enterprise Cyber Risks and reviewing regularly with Enterprise risk and the risk committee.
- Deliver programs to raise cyber awareness and effect cyber behavioural change across UNSW.
- Lead the implementation and maintenance of the DISP compliance as required.
- Develop and implement UNSW cyber strategy, enterprise security architecture design and information security policy framework, as well as contributing to and aligning to university policies and approaches that are appropriate to manage existing and emerging cyber risks.
- Ensure that the cyber security objectives of the University Foreign Interference Guidelines are met by the UNSW cyber strategy.
- Build productive relationships with related functions, such as Legal, Privacy, UPP, UNSW Cyber School and lead the provision of authoritative advice and guidance on the requirements for cyber security controls in collaboration with those areas.
- Maintain the identity strategy based on UNSW business needs to drive the ongoing development and design of the identity architecture to deliver capabilities to support the current and future needs of UNSW.
- Review new business proposals and provides specialist advice on cyber security issues and implications to UNSW.
- Be accountable for the content and effectiveness of the NWOW cyber guardrails,
- Drive to closure identified exposures and vulnerabilities by tasking owners with activities to remediate and control those exposures

- Represent UNSW in industry forums to provide thought leadership across the sector.
- Implement the UNSW Health and safety management system within your area of responsibility.

SELECTION CRITERIA

- Degree in computer science or related discipline (e.g. ITIL Master), with proven experience in technical field, ideally within a large complex organisation.
- Demonstrable experience in a Cyber Security leadership role for at least 5 years in a comparable organisation
- A proven approach to developing and delivering a risk-based approach to Cyber Security.
- Demonstrable working knowledge of a broad range of security technologies e.g. encryption, multifactor authentication, endpoint protection, IDS/IPS, PCI, access control, vulnerability management toolsets, malware defences, protective monitoring, physical security controls
- Demonstrated experience in formulating and implementing cyber-security strategy in complex organisations.
- Highly developed networking, interpersonal and stakeholder management skills with an ability to influence senior management and ability to explain technical matters to non-technical users.
- Ability to adapt to a fast-moving IT landscape and keep pace with latest thinking and new security technologies
- Strong interpersonal skills and a proven ability to engage at all levels of an organisation, up to Board and CEO level.
- Ability and capacity to direct and monitor the implementation and effectiveness of the safety management system.

It is not the intention of the position description to limit the scope or accountabilities of the position but to highlight the most important aspects of the position. The aspects mentioned above may be altered in accordance with the changing requirements of the role.