POSITION DESCRIPTION

Principal Cyber Security Architect

Position Summary

The Principal Cyber Security Architect will be responsible for developing, communicating, and maintaining Cyber Security transformation strategies, security architectures, and security roadmaps. This role will work across all program initiatives within the Cyber Security program and will partner with the UNSW Enterprise Architecture function and participate in the Architectural Working Group (AWG).

It will be important for the incumbent to align standards, frameworks and security with the overall UNSW business and technology strategy by designing architectures that define strong architectures to mitigate risk, identify the future state, and protect the wider digital and information assets of the University. As a very senior contributor, this role requires broad strategic thinking and engagement with the wider University stakeholders.

This role will be a collaborative position within the Cyber Security team and will peer with the UNSW Enterprise Architecture group. And this ability to work on cross-functional teams and across different parts of UNSW will be a key differentiator and success of the role judged by cross-functional achievements.

The objective of this position is to ensure UNSW can achieve its strategic objectives, while Securing enterprise information by determining security requirements; planning, implementing, and testing security systems; preparing security standards, policies, and procedures; mentoring team members.

The role reports to the Head of Cyber Strategy & Governance and has no direct reports

Accountabilities

Specific accountabilities for this role include:
• Drive the development, communication and implementation of Operational Technology / IT Cyber Security architecture, roadmaps, and standards, in alignment with UNSW Cyber Security Strategy & Enterprise Architecture.
• Provide expertise, leadership, guidance and support to solution architects, designers and project teams in the development, communication and full lifecycle management of enterprise aligned cyber security architectures.
• Identify security design/architecture gaps / flaws in existing and proposed architectures and recommend changes or enhancements.
• Engage with key stakeholders across the university to communicate the benefits of the enterprise cyber security architecture, plans and supporting the delivery of the organisational cyber security strategy.
• Work as part of a multi-discipline team supporting the development of long term technology strategies and roadmaps including definition of roadmap projects, costing and benefits.
• Provide expert, specialist advice to support transformation programs, providing strategy and services to support the resolution of conflicting demands and/or designs and initiatives that continue to mature this capability.
• Proactively identify and escalate potential risks and ensure security is appropriately addressed. Manage the development of risk management plans, establishment of risk controls and performance of risk mitigation activities.
• Leveraging and updating existing control reference patterns and developing new patterns to outline integration approaches, use-cases, re-use, and technical reference for Enterprise security capabilities.
• Development of high-level and detailed security requirements relating to project initiatives and security service catalogue.
• Understand and track emerging threats and technologies and their relevance to security architecture.
• Provide high level security architecture requirement to define RFI/RFP and liaise with the vendors.
• Ability to review new and existing Information Technology projects for information security compliance by developing, documenting, and communicating adherence to architecture, blueprints, components, standards and strategies.
• Guiding others in the practical application of security and risk management concepts, principles and strategies, and relevant industry standards.
• Ensure hazards and risks are identified and controlled for tasks, projects and activities that pose a health and safety risk within your area of responsibility.
• Align with and actively demonstrate the UNSW Values in Action: Our Behaviours and the UNSW Code of Conduct.
• Cooperate with all health and safety policies and procedures of the university and take all reasonable care to ensure that your actions or omissions do not impact on the health and safety of yourself or others.

Skills and Experience

• Tertiary qualification in a relevant field as well as minimum 10 years’ experience in Cyber Security with at least five years in security architecture role.
• Relevant industry certification(s), e.g. CISM, CISSP, SABSA, TOGAF, GIAC and/or relevant industry experience are highly desired.
• Knowledge of relevant industry frameworks relating to Operational Technology and Cyber Security (i.e. NIST, CIP, ISO/IEC 64223).
• Extensive experience and knowledge in cloud security including security compliance in Azure and AWS.
- Significant experience in developing, communicating, and maintaining cyber security architectures, roadmaps, policies and standards.

- Experience in shaping and driving the security design and deployment of major IT transformation programs from a cyber security perspective, including (but not limited to): network security architecture, desktop and server security architecture, cloud security and resilience architecture, threat and vulnerability management, centralised logging and threat correlation, IT Security architecture and segregation models.

- Experience with IAM, including strategies, trust models, and open standards (e.g. SAML, OAuth, OpenID Connect & SCIM) used to improve manageability, access governance, provisioning, information security, and privacy.

- Demonstrated ability to lead and influence other senior technical and business staff, without these people being direct reports.

- Solid understanding of application security vulnerabilities (OWASP top 10) and countermeasures to reduce related risks.

- High level written, verbal communication and interpersonal skills; along with the ability to negotiate, consult and persuade in a business and technical environment.

- Proven technical and interpersonal skills are required to develop sound communications options. An understanding of and commitment to UNSW’s aims, objectives and values in action, together with relevant policies and guidelines.

- Knowledge of health and safety responsibilities and commitment to attending relevant health and safety training.

About this document

This Position Description outlines the objectives, desired outcomes, key responsibilities, accountabilities, required skills, experience and desired behaviours required to successfully perform the role.

This template is not intended to limit the scope or accountabilities of the position. Characteristics of the position may be altered in accordance with the changing requirements of the role.

UNSW