Position Summary

The Application Security Lead will play a crucial role in strengthening the organisation’s security position by leading secure development lifecycle practise (SDLC). This role will collaborate closely with the Cyber Security team and use expertise to develop and drive practices that embed secure-by-design across the full technology stack for applications. This role leads application security compliance across the Student, Academic and Research domain.

The Application Security Lead role will lead the organisation with strong development processes and work with various teams and stakeholders to provide consultation and guidance across the business. This includes promoting awareness of the University’s internal and external environment for emerging cyber security threats and supporting the independent audits of cyber security controls.

This role reports into the Technology Manager and has no direct reports.

Accountabilities

Specific accountabilities for this role include

- Lead the development and implementation of application security best practice processes that ensure security throughout the application lifecycle.
- Provide expert guidance and leadership on secure development practices and technologies to IT teams and stakeholders across UNSW to embed security practices.
- Collaborate with the Cyber Security team to establish and advance sustainable secure coding processes, platforms, tools, monitoring, and automation including hands-on set-up and management of application security tooling.
• Lead a capability uplift and embed a culture of security across application teams through the development of standards, guidelines and identifying team needs and opportunities.
• Develop and deliver application development training with respect to security and guide the team autonomously on department strategy and approach.
• Mentor and support application development team to develop technical skills and ensure security compliance.
• Support the independent audit of cyber security controls on behalf of the University, including statutory audits completed by the Audit Office of NSW.
• Continually stay up to date and aware of legal, regulatory compliance and contractual obligations that are relevant to the University’s management of cyber security risk.
• Promote awareness of the University’s internal and external environment for emerging cyber security threats.
• Develop and improve metrics that drive security best practice and outcomes.
• 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

• Preferably 10+ years work experience in software engineering or related roles, at least 2 of which within a similar role focused on application security.
• In-depth understanding of the most common application security risks and demonstrated experience in secure development practices required to mitigate those risks (e.g., OWASP Top 10).
• Hands-on experience in designing, implementing, and managing secure software delivery pipelines by integrating application security tooling (such as SAST, DAST and dependency vulnerability management) into CI/CD pipelines.
• Understanding of architecture and security concerns specific to web technologies and frameworks (e.g., secure password storage, encryption, security headers, content security policy, CSRF, OIDC, OAuth2, hash algorithms, one-time codes, password reset, rate limiting, security logging, etc), API security and identity and authorisation standards.
• AWS and Azure security knowledge and experience desirable
• Strong problem-solving and analytical skills, with the ability to translate data into valuable information for management.
• Strong cyber security GRC fundamentals and knowledge of cyber security principles and practices.
• Excellent understanding of industry-wide security standards and compliance frameworks such as ISO 27001, NIST 800-53, CSA, Essential 8, PCI DSS, COBIT 5, Mitre ATT&CK etc.
• Relevant industry certification(s) such as SANS certifications, CEH, OSCP, CompTIA Security+, and cloud platform certifications such as AWS Security Speciality, Microsoft Azure (highly desirable).
• Excellent communication and interpersonal skills, with the ability to effectively convey complex security concepts to technical and non-technical stakeholders.
About this document

This Position Description outlines the objectives, desired outcomes, key responsibilities, accountabilities, required skills, experience and desired behaviors 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.