Position Description

Cyber Security Architect

Faculty/Portfolio	eSolutions
School/Centre	Infrastructure Services
Basis of Employment	Full-time (36.75 hours per week)
Primary Location of Work	Geelong Waterfront or Melbourne Burwood Campus
Classification	HEW 9
Reporting Line	Manager, Information Security and Risk

ABOUT DEAKIN

Deakin University is proud to be recognised as an organisation that offers a friendly, supportive and challenging working environment. Our staff are committed to making a genuine difference to people's lives through excellence in education and research. We acknowledge the importance of providing a dynamic and diverse working environment and offer variety in day-to-day roles as well as professional development opportunities to assist staff to grow and progress their careers. Deakin University staff have the opportunity to interact with colleagues from a diverse range of cultures and professional backgrounds, all of whom share a common interest in lifelong learning.

Deakin is Australia's sixth largest university and number one in Victoria for student satisfaction – a ranking of which we are very proud. Deakin University operates five campuses; the Cloud Campus, Melbourne Burwood Campus, Geelong Waurn Ponds Campus, Geelong Waterfront Campus, and the Warrnambool Campus. We have four corporate centres in Melbourne's CBD, and at the Burwood, Waterfront and Waurn Ponds campuses, as well as offices in India, China and Indonesia.

WHY WORK FOR OUR UNIVERSITY?

eSolutions

Benefits of working at Deakin

Deakin's Strategic Plan – LIVE Agenda

DEAKIN'S PROMISE TO EQUITY, DIVERSITY AND INCLUSION

At Deakin we value diversity, embrace difference and nurture a connected, safe and respectful community. Deakin is an Employer of choice for Gender Equality, a proud member of the SAGE Athena SWAN program seeking gender equity for Women in STEMM, and a bronze award holder in the Australian Workplace Equality Index for LGBTI inclusion. We strongly encourage applications from Aboriginal and Torres Strait Islander people and people of all cultures, abilities, sex and genders.

POSITION OVERVIEW

The Cyber Security Architect is responsible for designing, building, testing and implementing security systems for the protection of university systems and data. The role exists to reduce risk to Deakin, its staff, students and their information by the provision of security architecture and design services, and to also ensure Deakin meets its policy, legal and regulatory obligations.

The Cyber Security Architect designs security controls to ensure coverage of all critical portfolio processes, and to support the objectives and strategy of the business. It is the Cyber Security Architect's responsibility to liaise with the university portfolios, and Cyber Security teams to understand the business requirements and to design controls which enable the university to manage risk, and achieve its objectives securely.

Deakin eSolutions (DeS) is part of the Chief Digital Officer's portfolio and has oversight and management responsibility for all Information and Communication Technologies (ICT) used by Deakin University.

The position sits in the Cyber Security team within eSolutions. The position reports to the Manager, Information Security and Risk. The Cyber Security Architect will be a key member in a team responsible for the identification and delivery of initiatives to improve efficiency and effectiveness of security services to Deakin.

Additionally, the Cyber Security Architect will liaise with internal and external business and technology stakeholders, to provide leadership and guidance around security architecture approaches and practises to help Deakin realise its long term security strategy and roadmaps.

Key Relationships:

Internal	• All eSolutions teams • University project teams • University portfolios
External	• Technology vendors

PRIMARY RESPONSIBILITIES

- High-level stakeholder engagement skills and provides technical leadership and oversight across the Cyber Security team.
- Provide leadership to align standards, frameworks and security with overall business and technology strategy ensuring achievement of portfolio objectives
- Design, build and implement enterprise-class security systems for a production environment
- Identify and design security architecture elements to mitigate emerging security threats in align with Deakin's long-term security strategy and roadmaps.
- Define and maintain a framework of security patterns, blueprints, services and guardrails to empower the business to rapidly and safely innovate within a hybrid cloud environment.
- Provide strategic advice and high level guidance on security strategies to manage identified risks and ensure adoption and adherence to standards.
- Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems.
- Contributes to the development of information security policy, standards and principles.
- Establishing disaster recovery procedures and conducting a breach of security drills.
- Assist the Manager, Information Security and Risk and other team members as required undertake the functions of the team.
- Any other duties as directed, commensurate with the scope and classification of the position

ABOUT YOU

To be successful at Deakin you are willing to enthusiastically embrace the Deakin Offer and Promise as expressed in the Deakin University Strategic Plan, and must share the University's values.

You will be a person who is ambitious for Deakin University's success and optimistic about its future; and will display diligence, have great resolve and a focus on producing results.

SELECTION CONSIDERATIONS

Qualifications and Experience:

- A degree in Information Technology, Computer Science or related field.
- Industry security qualifications such as CISSP, CISM, SABSA or ISSAP are desirable
- High level of understanding of security operations and technology architectures.
- 5 - 10 years working experience in security, risk management, assurance management, designing, building and running technology services in alignment with security best practice.
- Experience in facilitating outcome focused risk workshops with a range of technical and business stakeholders.
- Proven technical experience across a wide variety of technologies such as digital, cloud, networks, applications and platforms.
- Demonstrated experience in the development and governance of information security and network architectures in complex environments.
- Experience in security threat and risk assessments, policy, architecture and design.
- Up to date with cloud and emerging technologies and associated risks and opportunities.
- Experience with frameworks such as NIST CSF, ISO27001/2, ISO 3100, TOGAF, SABSA.
- Experience working with agile delivery methodologies (desirable).

Capabilities and Personal Attributes:

- High level communication skills, including excellent conceptual, analytical problem solving reporting and presentation skills and the ability to write compelling and effective business cases.
- Demonstrated interpersonal skills, including an ability to build and establish strong relationships, negotiate, consult and persuade and to represent the Portfolio within the University.
- Demonstrated self-motivation and ability to work independently but also collaboratively as a team leader to achieve common goals whether internal to the Portfolio or wider the University or external community.
- High level of responsiveness to changing priorities and to implement and manage change in the workplace and proven capacity to work well in a highly pressured environment.
- Ability to interpret and apply University administrative policies and procedures to a range of work related issues.
- Demonstrate the ability to exercise sound judgment, initiative, diplomacy, tact and discretion as well as proven experience handling sensitive and personal information in a confidential and appropriate manner

SPECIAL REQUIREMENTS

- It is an inherent requirement of the role to accommodate a flexible work schedule, including out of hours work to fulfil the operational needs of this position. For this reason, annual leave may not be approved during peak times of work.
- Travel to other campuses of the University will be required on a regular basis. A commitment to understanding the need for, and ensuring the confidentiality of the sensitive nature of information to which the position may have access.

DISCLAIMER

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.