

POSITION DESCRIPTION

Position Title	Senior Lead, IT Security		
Organisational Unit	Information Technology		
Functional Unit	IT Security and Infrastructure Services		
Nominated Supervisor	National Manager, IT Security and Infrastructure Services		
Classification	HEW 9		
CDF Level	CDF2L	Position Number	10613470
Attendance Type	Full Time	Date reviewed	11-JUN-2026

ABOUT AUSTRALIAN CATHOLIC UNIVERSITY

ACU has a bold vision for its future. Our Vision 2033 is our landmark statement of strategic direction for ACU's mission as a Catholic university to constitute a 'Christian presence in the university world confronting the great problems of society and culture'. Our mission is to help shape the coming generations in Australia and beyond, by enabling flourishing lives, fostering thriving communities, and building a more ethical future.

Our Catholic mission informs everything we do – challenging us to respect the dignity of the human person, serve the common good, and embed ethical and social justice considerations throughout our teaching and research. We strive to live our core values of truth, excellence, and service.

We are a publicly funded university, and while we are young, we have grown significantly and we and we are making our mark: we are one of the largest university contributors to the care economy in Australia and rank among the top universities worldwide. We have seven campuses around Australia, more than 200 partner universities on six continents, and a campus in Rome, Italy.

We prioritise our staff, supporting their growth with a positive culture, generous leave, and flexible work arrangements. We invite all staff to engage with our mission in whatever way is most meaningful to them – whether as Catholics, as members of other churches and faiths, or as people with no religious affiliation but who are willing to embrace our vision, mission and strategic direction. We continue to invest in our facilities and workplaces and actively involve staff in shaping the future direction of the organisation.

For further information about the university please refer to ACU's [organisational structure](#).

ABOUT INFORMATION TECHNOLOGY

Operating within the ACU's Corporate Services Portfolio, the Information Technology Directorate's core purpose is to deliver and manage the technology capabilities required to enable learning, teaching, research and business support functions across ACU to achieve their strategic and operational objectives and to foster a culture of digital innovation that enables the advancement of ACU's offer and execution, student experiences, and its industry partnerships.

The Information Technology Directorate is led by the Chief Information and Digital Officer (CIDO) and a leadership team of five direct reports, each representing distinct areas of focus required to realise its purpose, namely, Enterprise Capabilities, Data Excellence, Cyber Security, Service Delivery, and Digital Innovation & Change.

ABOUT CYBER SECURITY SERVICES

Cyber Security Services works to protect ACU against the evolving landscape of cyber-threats, through a risk-based approach.

The functional group consists of two teams that work closely together:

- Enterprise Information Security provide assurance to ACU of protection against cyber-threats through setting a robust IT security and risk management strategy, assessment of threats, operation of cyber security services, and continuous improvement.
- The Cyber Security Program team undertakes a continually evolving program of work in order to deliver significant improvements to ACU's cyber security and identity posture.

POSITION PURPOSE

The Senior Lead, IT Security is responsible for leading and developing a high-performing team of internal and external resources/partners delivering secure, resilient and compliant IT Security services across the university.

The role provides strategic and technical leadership in cybersecurity, including risk management, threat detection and response, security governance, and the adoption of industry best practice frameworks and standards. It ensures the effective day-to-day coordination and performance of managed security services providers, while collaborating with senior stakeholders, IT teams, architects and vendors to deliver integrated and secure technology solutions.

The position drives continuous improvement in service quality, strengthens the organisation's security posture, and aligns security initiatives with the university's strategic objectives to support teaching, learning and business outcomes.

KEY RESPONSIBILITIES

Introduction

A number of frameworks and standards express the University's expectations of the conduct, capability, participation and contribution of staff. These are listed below:

- [ACU's Vision 2033](#)
- [Catholic Identity and Mission](#)

- Code of Conduct for all staff
- ACU Capability Development Framework
- ACU Staff Enterprise Agreement 2022-2025
- ACU Staff Reconciliation Action Plan

The Capability Development Framework describes the core competencies needed in all ACU staff to achieve the university's strategy and supports its mission.

Responsibility	Scope
People and resource management: • Lead a team of technical experts providing support across IT Security activities, including building capability, setting and managing team and individual performance objectives, resource planning and recruitment of high-performing staff and consultants where required. • Responsible for capacity planning and managing resources to balance workload. • Responsible for the day-to-day coordination and operational oversight of the managed security services provider (MSSP), ensuring service delivery aligns with contractual obligations, performance expectations, and organisational security requirements.	The position mainly contributes to activities; outcomes and goals within their immediate team or work unit
Strategy and stakeholder engagement: • Liaise with the National Manager, IT Security and Infrastructure Services, as well as other senior stakeholders to make strategic recommendations in the adoption of innovative IT Security and Infrastructure Services to improve business and teaching/learning processes, communication and collaboration. • Contribute to the development of strategic proposals and programs of work that demonstrate clear alignment to the university and the directorate's strategic goals. • Provide consultancy to and collaborate with internal and external stakeholders, IT teams and vendors to ensure the high quality and availability of secure application and platform services to the university community, as required to plan and deliver integrated services.	The position contributes to activities; outcomes and goals; that are implemented and have impact across the University
Technology competency: • Lead and provide expertise in all areas of IT Security and Infrastructure Services, with a particular focus on cybersecurity, risk management, threat detection and response, and security governance. • Provide technical subject matter expertise to ensure service offerings are aligned to our technology footprint.	The position contributes to activities; outcomes and goals; that are implemented and have impact across the University
	The position contributes to activities; outcomes and goals; that are

Responsibility	Scope
Adoption of frameworks, industry standards and best practice: • Provide technical leadership and subject matter expertise in the adoption of industry best practice security frameworks, methodologies and standards to improve and enhance service offerings and outcomes, through the automation and implementation of appropriate tools and processes that enable delivery of business objectives.	implemented and have impact across the University
Governance and Reporting: • Design and lead improvements to the quality of IT service performance and reduce operational and security risk. • Deploy and manage various systems and tools to monitor service utilisation trends, performance, vulnerabilities and security threats and provide leadership in incident and problem resolution, including security incidents. • Coordinate and oversee security assessments, including vulnerability assessments and penetration testing, new product/service risk assessments, ensuring activities are risk-based, effectively delivered by internal and external providers, and that identified vulnerabilities are promptly remediated to strengthen the organisation's security posture.	The position contributes to activities; outcomes and goals; that are implemented and have impact across the University
Cross team and business unit collaboration: • Work collaboratively with internal IT teams and Domain Enterprise Architects, within the IT Directorate and across the university, to deliver strategic and operational solutions and outcomes, enhance existing capabilities and roll out new security features as prioritised by the business owner.	The position contributes to activities; outcomes and goals; that are implemented and have impact across the University
Contribute to policy and process development: • Provide technical leadership to all stages of processes related to IT Security to ensure compliance with relevant technical standards, regulatory requirements and achievement of documented security controls and requirements.	The position mainly contributes to activities; outcomes and goals within their immediate team or work unit

HOW THE ROLE OPERATES

The position manages complex; difficult or challenging matters/issues/tasks on a regular basis; These matters are often impacted by internal/external factors (technical; policies and procedures; industrial; funding; academic).
The position is expected to demonstrate critical thinking to make recommendations; to meet changing demands; and provide business aligned solutions.

The position will need to influence and win the support of others to achieve mutually beneficial outcomes.

The position manages a geographically dispersed team.

SELECTION CRITERIA

Qualifications, skills, knowledge and experience:	• Qualification - Postgraduate qualification in Information Technology, Cyber Security or a related discipline, and/or extensive relevant experience. • Experience - Demonstrated experience leading and developing teams and delivering IT Security operational ("Business as Usual") and project-based initiatives. • Experience - Demonstrated experience in applying security best practice, frameworks and methodologies across the design, implementation, testing and operational management of secure, scalable and resilient solutions. • Experience - Experience in delivering and operating enterprise IT Security services, including threat detection and response, risk management, security operations, and governance, within complex environments. • Experience - Demonstrated experience in implementing and managing contemporary security technologies and services, including identity and access management, endpoint and network security, and cloud security controls. • Experience - Demonstrated experience building and maintaining security automation, orchestration and monitoring capabilities, including integration with security operations and managed security services. • Knowledge - Strong understanding of contemporary cyber security frameworks, standards and best practices (e.g. ISO 27001, NIST, Essential Eight), preferably within a higher education or similarly regulated environment. • Experience - Excellent written and verbal communication skills, with the ability to translate complex security concepts into clear, actionable insights for diverse audiences, and proven experience engaging, influencing and collaborating with senior stakeholders, technical teams and external partners.
Core Competencies:	• Demonstrate confidence and courage in achieving ACU's Mission, Vision and Values by connecting the purpose of one's work to ACU's Mission, Vision and Values. • Display openness and resilience, inspire others to change and act to make change happen with ACU's strategic goals and Mission at the heart of all outcomes. • Keep stakeholder interest at the core of ACU business decisions and ACU service excellence as a top priority. • Communicate with purpose. Gain the support of others for actions that benefit ACU. Negotiate for mutually beneficial

	outcomes that are aligned with the Mission, Vision and Values of the University. • Coach and develop self and others through setting clear expectations, managing performance and developing required capabilities to establish a culture of learning and improvement.
Essential Attributes:	Demonstrated commitment to cultural diversity and ethical practice principles and demonstrated knowledge of equal employment opportunity and workplace health and safety, appropriate to the level of the appointment.
Working with Children and vulnerable adults check	This role does not require a Working with Children Check.
Pre-employment declaration and background check	Preferred candidates will be required to complete mandatory pre-employment declarations and background checks, including those related to gender-based violence and foreign interference, in line with ACU's compliance requirements.

REPORTING RELATIONSHIPS

For further information about the structure of the University, refer to the Organisation Chart

<https://www.acu.edu.au/about-acu/leadership-and-governance/leadership/organisational-structure>