

POSITION DESCRIPTION

Position Title	Technical Lead, Cyber Program		
Organisational Unit	Information Technology		
Functional Unit	IT Security and Infrastructure Services		
Nominated Supervisor	Senior Lead, IT Security		
Classification	HEW 8		
CDF Level	CDF1	Position Number	10613481
Attendance Type	Full Time	Date reviewed	15-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,
 PD_Technical Lead, Cyber Program

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 Technical Lead, Cyber Program is responsible for providing technical leadership to the planning, coordination, and delivery of the university's cyber security program, ensuring initiatives are aligned to strategic objectives, risk priorities, and regulatory obligations. Working under the direction of the Senior Lead, IT Security and in partnership with the Project Manager, Cyber Program, the role provides technical leadership across a portfolio of cyber security initiatives, collaborating with stakeholders, faculties, and business units to translate organisational needs into practical, fit for purpose security 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
Provide expert technical leadership across cross functional teams to shape, coordinate, and deliver cyber security program initiatives that address complex business and operational requirements and align with organisational strategy.	The position contributes to activities; outcomes and goals; that are implemented and have impact across the University
Continuously monitor emerging threats, vulnerabilities, and industry trends to inform program priorities, recommend	The position contributes to activities; outcomes and goals; that are

Responsibility	Scope
strategic improvements, and strengthen the maturity of the organisation's cyber security capability.	implemented and have impact across the University
Provide expert leadership across key cyber security domains, including cloud security, identity and access management (IAM), network security, endpoint protection, and security operations, ensuring cyber security program initiatives are secure by design and sustainable in operation.	The position contributes to activities; outcomes and goals; that are implemented and have impact across the University
Drive the integration of cyber security requirements into risk management, business continuity, disaster recovery, and project delivery practices, ensuring security is embedded consistently across platforms, services, and programs of work.	The position mainly contributes to activities; outcomes and goals within the faculty/directorate/organisational unit
Other duties as required, that commensurate with the role and level.	The position mainly contributes to activities; outcomes and goals within their immediate team or work unit

HOW THE ROLE OPERATES

The position will have the freedom to implement changes to policies; processes and procedures based on their expertise.
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.
This position does not have managerial responsibilities.

SELECTION CRITERIA

Qualifications, skills, knowledge and experience:	• Qualification - Bachelor's degree in Information Technology, Computer Science, Cyber Security, Engineering, or a related discipline. Relevant industry certifications in information security and risk management (e.g. CISSP, CISM, CCSP, Microsoft Security, AWS Security, or similar) are highly regarded. • Experience - Extensive experience in providing technical leadership to and delivering cyber security programs, initiatives, or uplift activities within complex organisational environments, including responsibility for strategic planning, governance, risk reduction, and coordination of multiple workstreams. • Knowledge - Strong knowledge of enterprise cyber security practices across cloud and hybrid environments (e.g. Azure, AWS, GCP, Palo Alto, Zscaler etc), including secure architecture, identity services, networks, applications, and data protection controls. • Experience - Demonstrated experience delivering cyber security initiatives involving technologies and controls such as identity and access management (IAM), SIEM/SOAR, endpoint detection and response (EDR), vulnerability management, network security, and logging and monitoring platforms. • Knowledge - Solid understanding of security frameworks and best practices (e.g. NIST, ISO 27001, Essential Eight), including governance, risk management, secure delivery practices, continuous monitoring, incident response, and control uplift.
--	--

	• Skill - Highly developed analytical and problem-solving skills, with the ability to identify complex cyber security issues, evaluate strategic options, and lead effective responses across multiple systems, teams, and delivery partners. • Skill - Strong communication, stakeholder engagement, and leadership skills, including the ability to influence outcomes, translate complex cyber security issues into clear business impacts, and build alignment across technical and non-technical stakeholders.
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. • Keep stakeholder interest at the core of ACU business decisions and ACU service excellence as a top priority. • Work collaboratively internally and externally to ACU to capitalise on all available expertise in pursuit of excellence. • Plan work activity, prioritise time and resources using established ACU processes and technology to achieve optimum efficiency and effectiveness. • Make informed, evidence-based decisions by sourcing and interpreting University and business information.
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>