

POSITION DESCRIPTION

Position Title	IT Security Specialist		
Organisational Unit	Information Technology		
Functional Unit	IT Security and Infrastructure Services		
Nominated Supervisor	Senior Leader, IT Security		
Classification	HEW 8		
CDF Level	HEW 8 CDF1	Position Number	10610617
Attendance Type	Full Time	Date reviewed	10-AUG-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_IT Security Specialist

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 IT Security Specialist is responsible for designing, implementing, and managing enterprise security controls and secure infrastructure to protect information assets, manage risk, and ensure compliance with regulatory and industry standards, while aligning technology initiatives with the university's strategic objectives. Working under the direction of the Senior Lead, IT Security, the role collaborates with stakeholders, faculties, and business units to identify security risks and translate business and technical requirements into secure, fit-for-purpose solutions that support operational and strategic goals. The specialist provides technical leadership and expert guidance across key security domains, including incident response, threat management, risk assessment, and business continuity, while continuously monitoring emerging threats and technologies to drive improvements and ensure systems and services remain secure, resilient, and aligned with best practices.

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 security leadership across cross-functional teams to understand complex business and operational requirements and translate them into secure, resilient, and scalable solutions aligned with organisational strategy.	The position contributes to activities; outcomes and goals; that are implemented and have impact across the University
Design, implement, and maintain enterprise security architectures and controls, ensuring protection of systems, data, and services while meeting regulatory obligations and industry best practices.	The position mainly contributes to activities; outcomes and goals within the faculty/directorate/organisational unit
Continuously monitor and assess emerging threats, vulnerabilities, and technology trends, proactively recommending improvements to strengthen the organisation's security posture.	The position contributes to activities; outcomes and goals; that are implemented and have impact across the University
Provide expert guidance across security domains, including cloud security, identity and access management (IAM), network security, endpoint protection, and systems integration, ensuring solutions are secure by design and operationally sustainable.	The position mainly contributes to activities; outcomes and goals within the faculty/directorate/organisational unit
Engage with senior stakeholders and service owners to assess security posture, identify risks, evaluate mitigation strategies, and provide evidence-based recommendations focused on reducing organisational risk and improving resilience.	The position contributes to activities; outcomes and goals; that are implemented and have impact across the University
Lead and support the investigation, analysis, and resolution of security incidents and vulnerabilities, ensuring the integrity, availability, and confidentiality of critical systems and services.	The position contributes to activities; outcomes and goals; that are implemented and have impact across the University
Contribute to and guide risk management, business continuity, and disaster recovery planning, ensuring security considerations are embedded across all platforms and services.	The position contributes to activities; outcomes and goals; that are implemented and have impact across the University
Provide operational oversight and governance of the Managed Security Services Provider (MSSP) to ensure delivery of agreed security services aligns with organisational requirements, service level agreements (SLAs), and security objectives. Monitor provider performance across key security functions including threat detection, incident response, vulnerability management, and monitoring services, ensuring timely and effective outcomes. Act as the primary escalation and coordination point for security incidents involving the MSSP, validating response actions and ensuring appropriate remediation.	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 - Possession of a 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 delivering and supporting enterprise information security solutions within complex organisational environments, including responsibility for security controls, incident response, vulnerability management, and risk remediation initiatives. • Knowledge - Strong knowledge of enterprise cloud security and hybrid environments (e.g. Azure, AWS, GCP, Palo Alto, Zscaler etc), including secure configuration of identity services, networks, applications, and data protection controls. • Experience - Demonstrated experience in managing and overseeing managed security services providers (MSSPs), including monitoring service performance against SLAs and KPIs, with the proven ability to establish effective vendor relationships, conduct service reviews, and drive continuous improvement, while ensuring alignment with organisational security policies, risk management frameworks, and regulatory obligations. • Experience - Demonstrated experience implementing and integrating security platforms and controls, including identity and access management (IAM), SIEM/SOAR, endpoint detection and response (EDR), vulnerability management, network security, and logging and monitoring solutions. • Knowledge - Solid understanding of security best practices and frameworks (e.g. NIST, ISO 27001, Essential Eight), including secure DevOps (DevSecOps), continuous monitoring, incident response, threat management, and change control processes. • Skill - Highly developed analytical and problem-solving skills, with the ability to identify, assess, and respond to complex security threats and vulnerabilities across multiple systems, teams, and vendors. • Skill - Strong communication and stakeholder engagement skills, including the ability to translate technical security risks and controls into clear, actionable insights for non-technical and senior stakeholders.
Core Competencies:	• 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>