

POSITION DESCRIPTION



ICT Cloud & Cyber Security Engineer

Business Support Services

About Jesuit Social Services

Jesuit Social Services is a social change organisation working to build a just society where all people can live to their full potential. We do and we influence. We accompany people and communities to foster and regenerate the web of relationships that sustain us all – across people, place and planet; and we work to change policies, practices, ideas and values that perpetuate inequality, prejudice and exclusion.

Our Vision

Building a Just Society

Our Mission

Standing in solidarity with those in need, expressing a faith that promotes justice.

Our Values

- Welcoming – forming strong, faithful relationships
- Discerning – being reflective and strategic in all we do
- Courageous – standing up boldly to effect change

Our Purpose

We work to build a just society where all people can live to their full potential – by partnering with community to support those most in need and working to change policies, practices, ideas and values that perpetuate inequality, prejudice and exclusion.

Position details

POSITION TITLE:	ICT Cloud & Cyber Security Engineer
PROGRAM:	Finance and Organisational Processes
LOCATION:	Richmond
REPORTING RELATIONSHIPS:	This position reports directly to the ICT Manager
EFFECTIVE DATE:	January 2026

Position Purpose

The ICT Cloud and Cyber Security Engineer is responsible for designing, implementing, and maintaining

secure cloud infrastructure and cyber security measures across the organisation. This role ensures the confidentiality, integrity, and availability of cloud-based systems and data, proactively defending against evolving cyber threats and ensuring compliance with regulatory standards. The engineer collaborates with JSS internal ICT Team, JSS ICT managed service provider and business teams to integrate security into all aspects of cloud and ICT operations.

Program Purpose

Central Office

Jesuit Social Services engages with people from diverse backgrounds experiencing complex problems, including those associated with mental illness, substance misuse, family breakdown, offending behaviour, homelessness, unemployment, poverty and social exclusion.

Jesuit Social Services operates a range of programs for disadvantaged young people, families and communities from various operational sites.

The Finance and Organisational Processes team is responsible for financial administration, human resources, operations, quality, risk and compliance, ICT and payroll of Jesuit Social Services and is located at Central Office in Richmond.

Duties of the position

- Design, Implementation & Architecture
 - Architect secure cloud solutions (e.g. AWS, Azure, Microsoft 365) and integrate security controls into cloud environments.
 - Design and deploy secure cloud infrastructures and applications, adhering to industry-standard security frameworks.
 - Automate security processes and integrate security into operational workflows.
 - Select and configure appropriate cloud services and security tools to minimise risks, vulnerabilities and threats.
- Monitoring, Detection, and Incident Response
 - Monitor cloud environments for security threats, vulnerabilities, and incidents using advanced security tools (SIEM, IDS/IPS, firewalls).
 - Conduct vulnerability assessments, penetration testing, and risk analyses on cloud systems and applications.
 - Respond to security incidents, perform forensic analysis, and participate in cyber incident management and reporting.
 - Develop and maintain incident response plans, including disaster recovery and business continuity strategies.
- Compliance, Governance, and Risk Management
 - Ensure cloud environments meet security and regulatory requirements (GDPR, HIPAA, SOC 2, ISO 27001, Essential Eight).
 - Conduct regular audits, compliance checks, and update security measures to align with evolving standards.
 - Maintain a digital asset register and ensure alignment with organisational risk management frameworks.

- Manage supplier risk and cloud services risk assessments, including third-party vendor compliance.
- Identity, Access, and Data Protection
 - Manage identity and access controls, ensuring only authorised users can access cloud resources.
 - Implement and maintain encryption, tokenisation, and other data protection mechanisms for sensitive information.
 - Enforce multi-factor authentication and password management processes across all cloud-based services.
- Security Operations and Continuous Improvement
 - Proactively hunt for threats and indicators of compromise (IOC) within cloud environments.
 - Stay current with emerging cloud security threats, technologies, and mitigation strategies.
 - Regularly report on the status of cloud security, including breaches, vulnerabilities, and compliance metrics.
 - Participate in ongoing cyber security training, awareness programs, and professional development.
- Collaboration, Training, and Stakeholder Engagement
 - Work with cross-functional teams (IT, development, business units) to identify and remediate security issues.
 - Provide security training and guidance to development and operations teams.
 - Collaborate with third-party vendors and service providers to ensure security requirements are met.
 - Report to governance committees (Risk and Finance Committee, Governance Committee) on cyber security strategy and activities.
- Advanced and Strategic Duties
 - Lead strategic cloud security initiatives and contribute to the development of cyber security strategy and workplans.
 - Advise on procurement and outsourcing, ensuring security compliance in contracts and vendor relationships.
 - Develop and maintain security documentation, policies, and procedures for cloud operations.
 - Support business continuity and disaster recovery planning, including testing and improvement cycles.

Key Selection Criteria

Required:

- Bachelor's degree in computer science, Information Security, Cybersecurity, or related field.
- Proven experience in cloud security engineering or a related discipline.
- Hands-on expertise with cloud platforms (AWS, Azure, Microsoft Intune, Microsoft 365) and their security features, configuration, backup and ongoing architecture.
- Previous experience with Microsoft Intune, Microsoft Defender and related endpoint management, configuration and protection.
- Familiarity with regulatory frameworks and compliance standards (RFFR, ISO 27001, Essential 8, NIST).
- Experience with implementing and aligning to industry cyber security standards e.g. ISO27001, NIST, Essential 8)
- Current knowledge of cyber security incident, SIEM management, threat / vulnerability detection and response functions.
- Strong understanding of identity and access management (IAM), encryption, and secure software development practices.

Desirable

- Previous experience working for a not-for-profit organisation.
- Multi-site, multi service shared service deliverable framework exposure
- Experience working with and managing external managed service providers
- Hands on practice managing significant technology change across varying business functions, internal teams and external service providers.

Key Performance Indicators

- JSS technology delivery and availability against underlying SLA's
- Contribution to management of technology ecosystem to maintain required information security standards
- Threat Detection: Support efforts to ensure security threats are identified and mitigated.
- Incident Response: Assist in the containment and resolution of cyber security incidents.
- Vulnerability Exposure: Help ensure security weaknesses are addressed within required timeframes.
- Patch Compliance: Participate in maintaining systems with up-to-date security patches.
- Audit Pass Rate: Contribute to successful completion of security and compliance audits.
- Risk Register Updates: Aid in the regular review and update of security risks.

Key responsibilities of Jesuit Social Services Employees

Service delivery/ Practice Framework

- Engage and build positive and constructive relationships with internal and external stakeholders
- Deliver services consistent with shared services guidelines, relevant legislation and funding agreements
- Communicate clearly with others

- Manage competing priorities in a high-volume work environment
- Fulfil the reporting and administrative requirements associated with the position
- Other duties as required.

Teamwork and supervision

- Work effectively as part of a team, contributing to group outputs
- Actively participate in regular supervision with the line manager, staff meetings and professional development opportunities.

Continuous Improvement and Professional Standards

- Demonstrate a commitment to own learning and development
- Commitment to risk management and continuous quality improvement processes
- Compliance with relevant legislation, Code of Conduct, policies and procedures of Jesuit Social Services

Diversity, inclusion and culture

- Always demonstrate respect and acceptance of diversity and provide culturally appropriate support to all including Aboriginal and Torres Strait Islander peoples and those who identify as LGBTQIA+
- Interact with staff, participants and other stakeholders in a manner that is inclusive, respectful and non-discriminatory

Mandatory Position Requirements

- Current National and International (where required) Police Check
- Current Employee Working with Children Check
- Valid and current Australian Drivers Licence
- Proof of eligibility to work in Australia

Safeguarding Children and Young People

Jesuit Social Services takes child protection seriously, we undertake a range of checks and processes to ensure safeguarding of children, and you are required to meet the behaviour standard outlined in our Code of Conduct.

Conditions of Employment

Conditions of employment are in accordance with the current Jesuit Social Services Collective Agreement and Jesuit Social Services Policy & Procedures, including the Code of Conduct.

Employee Acknowledgement

I, _____ (please print name) acknowledge that I have read and understood the contents of this position description.

Employee Signature

Date: _____

Position Description Approved by:

**ED Finance and Organisational
Processes**

Position Description Review Date

