Parliament of South Australia

Joint Services Division

Position Title:	Technical Specialist	**Location:**	Parliament House
Classification:	ASO6	**Reports to:**	Team Leader, Technology Services
Entity/Division:	Joint Services	**Direct Reports:**	0
Business Unit:	PNSG	**Job Status:**	Temporary < 6 months

ABOUT US

The Joint Parliamentary Service Committee (JPSC) is a Standing Committee of the Parliament. It consists of the President of the Legislative Council, the Speaker of the House of Assembly and two Members from each House. The JPSC is responsible for the administration of the Joint Parliamentary Services.

The JPSC is responsible for the administration of the Joint Parliamentary Service (JPS) Divisions such as the Parliamentary Library Division, the Catering Division, Hansard, and the Joint Services Division (including PNSG, People and Culture, Finance and Building Services).

PNSG is a business unit within the Joint Services Division that provides critical Parliamentary Information, Communication and Technology (ICT) infrastructure, functions and requirements to a broad customer base including Members of Parliament, Electorate Offices and the Parliament of South Australia.

KEY OBJECTIVES

The Technical Specialist – Server is accountable to the Team Leader, Technology Services to to deliver a range of specialised technical services supporting secure, reliable and high-performing ICT infrastructure across the Parliamentary environment, including:

- Provision and support of enterprise server, cloud and infrastructure platforms, ensuring performance, availability and resilience across Parliamentary systems.
- Management of cyber security operations, including monitoring, incident response, and implementation of controls aligned with relevant frameworks and standards.
- Delivery of technical advice and contributions to projects and system improvements, supporting secure and scalable solutions that meet business needs.
- Collaboration with stakeholders and service providers to support effective service delivery, including participation in change, incident and problem management activities.
- Development and maintenance of technical standards, documentation and team capability, contributing to continuous improvement and compliance across the ICT environment.

RESPONSIBILITIES

ICT Systems, Projects and Service Delivery

- Plan, deliver and support complex ICT systems, services and change initiatives aligned to organisational objectives.
- Contribute to critical and/or state-wide operations requiring high levels of technical expertise and accountability.
- Resolve complex technical issues using innovative and practical solutions.

Technical Advice and Continuous Improvement

- Provide expert technical advice to stakeholders and contribute to strategic and operational decision-making.
- Conduct research and analysis of emerging technologies, trends and complex issues.
- Identify and implement improvements to systems, services and processes.

Cyber Security Operations and Assurance

- Monitor, investigate and respond to cyber security threats, incidents and breaches, including use of SIEM and related tools.
- Support security assurance activities including vulnerability assessments, audits and compliance reviews.
- Ensure systems and services align with required security frameworks, standards and risk mitigation strategies.

Governance, Risk and Compliance

- Contribute to ICT governance processes, including change, risk and audit activities.
- Develop and maintain system documentation, standards and controls to support secure and compliant operations.
- Support cyber security investigations and reporting, including eDiscovery activities where required.

Stakeholder Engagement and Capability Development

- Build and maintain effective working relationships with internal stakeholders, service providers and partners.
- Provide high-quality customer service and technical consultancy across the organisation.

- Mentor and support team members and contribute to cyber security awareness and training initiatives

KEY SELECTION CRITERIA

- Demonstrated experience administering complex server environments, including physical, virtual and cloud platforms (e.g. Windows Server, Active Directory, storage, backup and enterprise email systems).
- Proven expertise in enterprise cloud and security environments, including identity and access management, configuration deployment, SIEM, and secure access across public and private networks.
- Strong knowledge and application of cyber security principles, including risk management, security controls, incident response, and protection of information assets in a medium to large ICT environment.
- Demonstrated ability to analyse and resolve complex technical problems, providing practical, innovative solutions aligned with organisational objectives.
- Experience delivering high-quality ICT support and customer service, including stakeholder engagement, issue resolution, and adherence to change management and security processes.
- Experience contributing to ICT projects and technology deployments, including planning, implementation, risk management and progress reporting.
- Proven ability to contribute to governance, audit and compliance activities, including cyber security reviews, system audits and continuous improvement initiatives.
- Highly developed interpersonal and communication skills, with the ability to build effective relationships and work collaboratively with diverse stakeholders across technical and business areas.
- Strong organisational skills and attention to detail, with the ability to manage competing priorities, work autonomously, and maintain accuracy in a complex technical environment.

KEY RELATIONSHIPS/INTERACTIONS

Internal:

- Team Leader, Technology Services (line manager).
- Executive Officer, Joint Parliamentary Service.
- Clerk of the Legislative Council.
- Clerk of the House of Assembly.
- PNSG team members.

- Finance Section, Joint Parliamentary Service.
- Chief Officers and managers of Joint Parliamentary Service.

External:

- Contractors
- Members of Parliament
- DTF Electorate Services

QUALIFICATIONS

- Relevant technical knowledge and/or certifications, such as Microsoft, Azure, M365, virtualisation, storage or security technologies, and familiarity with frameworks such as ACSC Essential Eight, ISO27001 or ITIL (desirable).

PRE-EMPLOYMENT SCREENING REQUIREMENTS

- All appointments are subject to reference checks, pre-employment assessment, and National Police Clearance.
- The inherent requirements of the role and intrinsic risk(s) will be considered in assessing prior conviction notifications and declarations of misconduct in previous workplaces.

ADDITIONAL INFORMATION

- The appointment is made pursuant to the Parliament (Joint Services) Act and, while the provisions of the Public Sector Act do not apply to this position, public sector conditions apply, and entitlements are transferable.
- There may be a requirement to work outside of normal working hours.
- Any person who is, and is seen to be, active in political or electoral affairs and intends to carry on this activity may compromise the strict political neutrality of this position and could not be considered for appointment.
- Employees are required to comply with all health, safety and risk management policies and procedures of the Parliament and take all reasonable care that any actions or omissions do not impact on the health and safety of others in the Parliament precinct.
- Employees must observe the Parliament of South Australia Code of Conduct and comply with the Conduct Standards in the Code.

CERTIFIED CORRECT

Executive Officer Title: _____ Date: / /