PARLIAMENT OF SOUTH AUSTRALIA

JOB AND PERSON SPECIFICATION

Title of Position:	Senior Technical Specialist - Network	**Administrative Unit:**	Parliament of South Australia
		Division:	Joint Services Division
Classification Code:	ASH7	**Section:**	Parliamentary Network Support Group
Discipline Code:	ASH		
Career Code:			

Type of Appointment:

- Ongoing
- ✓ Temporary (term)
- Other

Position Number:	P48408
Position Created:	December 2021
Position Reviewed:	November 2023

Job and Person Specification Approval

All excluding senior positions

..../..../....
Secretary to the Joint Parliamentary Service Committee

JOB SPECIFICATION

1. Summary of the broad purpose of the position in relation to the organisation's goals (its expected outcome and how it is achieved).

The Senior Technical Specialist position resides within Parliamentary Network Support Group (PNSG) in the Joint Services Division of the Parliament of South Australia. The role undertakes a range of complex and critical technical activities, providing high level specialist technical skills in the planning, development, maintenance, problem resolution and support of the technology platforms and systems servicing Parliament and Electoral Offices.

This role involves the application of technical skills and competencies, including the ability to manage highly complex projects and work packages for system development, as well as undertaking fault diagnosis and problem resolution, across a range of technologies, which primarily includes LAN / WAN networks, firewalls / gateways (proxies), SIEM, IPS / IDS and relationship management with support vendors. These technologies are physical, virtual and cloud based.

The incumbent will need to take a collaborative and team-first approach and develop and maintain effective consultative and collaborative relationships with a diverse range of internal and external stakeholders and service providers.

Responsibilities include collaboration with the support team of server, backup, storage, configuration deployment, SIEM, mail, application, database environments and interoperability relationships, and with other peer team members.

This is a trusted role and is required to undertake duties such as the eDiscovery function requiring an elevated security clearance to Australian Government Protective Security Policy Framework (PSPF) Negative Vetting Level 1.

2. Reporting/Working Relations (to whom the person reports, staff for whom the person is responsible, and other significant connections and working relationships within the organisation).

Reports to: Team Leader, Technology Services

Direct reports: contract/project staff as required

- Liaises closely with PNSG's IT management team, including the Unit Manager, Team Leader Technology Services, Team Leader Client Services and Team Leader Business Systems to ensure solution designs incorporate appropriate functionality, cyber security controls and meet relevant standards.
- Builds close working relationships within PNSG and specifically within the Technology Services Team with peer Senior Technical Specialists and the Technical Specialists.
- Builds close working relationships with Parliament staff and the IT staff of other Parliament business units to ensure the business needs of Parliament are met while relevant cyber security controls are applied in accordance with the agreed ACSC Essential Eight Maturity Model strategies.
- Builds close working relationships with internal and external ICT Security providers to ensure service levels are met and appropriate controls are in place to secure Parliament assets.
- Engages with the broader IT and cyber security community through interest groups, vendor forums and across government working groups.

3. Special Conditions (such as non-metropolitan location, travel requirements, frequent overtime, etc.)

This role has been classified as a position of trust. The incumbent is subject to a satisfactory criminal history / record check in line with departmental and Parliamentary policies and procedures.

- The incumbent is required to:
  - work on a roster system for on-call and after-hours support
  - hold a current driver's license and be prepared to drive to meet business requirements
  - refrain from any kind of political activity or involvement in electoral affairs
  - maintain confidentiality regarding sensitive client information.
- Some intra/interstate travel involving overnight absences may be required.
- The incumbent will be required to participate in the Parliament's Performance Development Program and achieve performance targets as negotiated and mutually agreed with the Team Leader, Technology Services.
- The incumbent may be required to be assigned to other positions at the same remuneration level across the Parliament.

4. Statement of Key Outcomes and Associated Activities (group into major areas of responsibility/activity and list in descending order of importance)**.**

1) The Senior Technical Specialist is required to undertake a wide range of activities which may include all or any of the following:

- Initiating, planning and delivering significant assigned agency programs, projects, systems and/or services that are consistent with the agency's objectives, including coordinating the implementation of change initiatives.
- Coordinating the resources and implementation processes for sensitive, innovative, critical or complex State-wide/service wide operations that demand a significant level of responsibility and decision making.
- Managing and motivating staff, clients and others in the achievement of difficult and sometimes conflicting objectives.
- Resolving complex issues with innovative solutions that are consistent with Agency objectives.
- Providing expert advice to senior management and external stakeholders regarding current relevant developments and their potential implications to agency policies and strategic plans.
- Leading, where required, high level research and analysis of complex and sensitive issues and/or policies.
- Contributing to a high standard of customer service for internal and external clients while ensuring cyber security controls and policies are complied with.
- Contributing to a safe, diverse and healthy work environment free from discrimination and harassment by working in accordance with legislative requirements, the Joint Parliamentary Service (JPS) employee Code of Conduct, equal employment opportunity and human resource policies, including Work Health Safety and Wellbeing requirements.
- Contribute to cyber security investigative processes by undertaking or participating in investigations into activities that breach security standards and policies, including activities of eDiscovery Officer when required.

2) Provide technical leadership and guidance across the department by ensuring:

- The provision of expert technical advice and support, contributing to the delivery of a range of projects, leveraging available technologies to achieve best practice and focussing on continuous improvement, to enable the Parliament and PNSG to achieve its strategic goals and objectives.
- Provision of technical leadership for a broad range of physical and cloud-based systems, ensuring risk assessments and information asset classification assessments are performed in conjunction with the business areas and appropriate policies, procedures and controls are adhered to, ensuring the security of sensitive information.
- Security standards and controls are maintained to the required tier levels to conform to the Parliament's agreed cyber security maturity model and levels of risk mitigation.
- Proactive management and monitoring of security threats, breaches and security incidents across supported Parliament systems, ensuring timely remedial action is taken to recover and prevent re-occurrence, including incident reporting, recording and monitoring via security incident and event monitoring (SIEM) systems and other available monitoring platforms.
- Participation in authorised penetration tests, vulnerability assessments, security audits, compliance reviews and other security assurance activities.
- Other team members are mentored as required.

3) **Contribute to the provision of quality technical and consultancy services to the department and oversee ICT security projects by:**

- Provision of ICT security advice and technical expertise with regards to security practices required to implement and introduce new services, including change processes relating to existing services.
- Provision of responsive, high-quality advice on information security practices to internal staff and PNSG business groups to enable them to meet their obligations to protect Parliament information assets.
- Review change advisory board requests for security impacts and compliance and contribute to problem management activities with security implications.
- Undertaking a consulting role and providing ICT security advice on corporate projects.
- Maintaining a strong awareness of current cyber security trends by maintaining a current understanding of emerging security threats; monitoring a range of industry information sources and networks, and initiating appropriate activities to protect Parliament assets.
- Undertaking research and evaluate emerging security technologies for suitability / usability within the department.

4) **Contribute to the efficient and effective communication of ICT security best practices and training by:**

- Participating in the ongoing education of staff and clients on current cyber security threats and good cyber security policy, practice and ensuring awareness of cyber security risks.
- Participating in and undertaking education and training programs on security policies, procedures and processes via Cyber Security Awareness and training programs that are developed and rolled out across the department.

5) **Contribute to the development and maintenance of Parliament systems and cyber security by ensuring:**

- Contribution to the development, implementation and maintenance of Cyber Security policies, standards, processes, templates, tools and techniques that are aligned with the agreed ACSC Essential Eight Maturity Model strategies and Parliament business objectives.
- System support documentation is developed and maintained, including identifying and outlining ways to address system risk exposures and produce baseline documentation and hardening standards compliant with reference architectures and standards.
- Regular Cyber Security reviews are conducted and documented for the information systems supported by PNSG on behalf of Parliament.
- The reporting and communication of cyber security events are managed appropriately and in a timely manner reported to PNSG stakeholders.
- Cost effective technical solutions are developed, documented, implemented and communicated in a timely manner in liaison with external service providers.

6) **Contribute to the effective risk, audit and mitigation activities of Information and Technology by ensuring:**

- I&T Risk, audit and mitigation activities relating to operational and cyber security matters are reported to PNSG leadership to ensure they are centrally and appropriately managed and resolved within agreed timeframes.

7) **The Parliament of South Australia adheres to the provisions of various Acts and associated legislation of the Equal Opportunity Act and Work Health and Safety Act**

Acknowledged by Applicant..... ...../...../.....

PERSON SPECIFICATION

Essential Minimum Requirements
(Those characteristics considered absolutely necessary)

Educational/Vocational Qualifications
Nil

Personal Abilities/Aptitudes/Skills
(Related to the job description, and expressed in a way which allows assessment)

1. Highly developed interpersonal skills, including a high degree of personal integrity and credibility.
2. Possess excellent administrative and organisational skills and an approach to work which emphasises accuracy and thoroughness.
3. Possess the ability to develop, manage and improve customer relationships with the divisions of Parliament and Members and their staff through the delivery of an effective ICT account management function including acting as a point of contact to key stakeholders in daily operations and in the event of major issues.
4. Ability to analyse complex problems, formulate solutions and implement appropriate and practical solutions.
5. Proven ability to work autonomously and collaboratively within a team environment, contribute to a culture of teamwork and shared responsibility for achieving results.
6. The ability to look ahead and think strategically to ensure flexibility of solutions to meet organisational needs now and also into the future.
7. Proven ability to contribute effectively in a team operating in a complex and technical environment, and to engender professionalism and cooperation at all levels.

Experience (Including community experience)

1. Extensive technical expertise in administering complex networks involving routing, switching, wireless, network and application security, mobile devices, TACACS+ and relationships with Active Directory leveraging CISCO or other comparable infrastructure and associated technologies.
2. Proven experience in management of LANs / WANs over wide geographical locations using TCP/IP and telecommunication infrastructure permitting secured access from public and private environments, utilising Virtual Private Networks (VPN), SDA, SDWAN, firewalls, / gateways (proxies).
3. Experience in support of enterprise scale environments demonstrating technical expertise and understanding of interoperability relationships between various systems and collaboration with other peer team members.
4. Demonstrated experience within a medium to large-scale information technology environment, particularly with respect to the application of information security principles to protect information assets.
5. Proven experience in contributing to the continual improvement of work procedures, policies and practices to meet the business, information technology and cyber security goals of an organisation.
6. Proven successful experience building strong/constructive relationships and networks including a proven capability to communicate and liaise effectively, consult and negotiate, with a range of stakeholders and customers across Government and industry at a technical and managerial level.
7. Experience in identifying operational and systems enhancement opportunities and in recommending appropriate action, in an information technology support environment.
8. Experience in acquiring and maintaining knowledge of relevant IT products and methods of IT support delivery.
9. Experience in conducting and contributing to security risk assessments, security architecture reviews and systems audit and risk mitigation reviews of network infrastructure for cyber security.

PERSON SPECIFICATION

Essential Minimum Requirements cont…
(Those characteristics considered absolutely necessary)

Experience (Including community experience) cont…

10. Experience in information technology customer service including, analysing problems and providing effective solutions while ensuring change management processes are followed and information and system security objectives are maintained.
11. Demonstrated experience in the implementation of complex technology deployments and project management of technology deployments including risk identification / management and progress reporting.
12. Successful record of identifying customer needs, developing service strategies, and providing quality customer service in either a public or private sector environment.
13. Demonstrated experience in the application of the relevant legislation, policies and procedures, including Code of Ethics, EEO and cultural inclusion.
14. Experience with the investigation and management of cyber security threats, breaches and security incidents.

Knowledge

1. Demonstrated knowledge of ICT networking and communication technologies and architectures with reference to cyber security, including:
    a. Extensive technical knowledge of LAN / WAN networks, firewalls / gateways (proxies), IPS / IDS environments
    b. Using packet tracing tools to identify causes of issues
    c. Patching and cable tracing
    d. Data security and encryption
    e. Security Incident and Event Management (SIEM).
2. Demonstrated knowledge of current cyber security technical controls and solutions through the application of risk management techniques to design, deploy and operate ICT services to deliver practical business solutions.
3. An understanding of the legislative requirements of the Work Health and Safety Act 2012.
4. An understanding of and ability to manage to the spirit and principles of ISO 3100 Risk Management.

DESIRABLE REQUIREMENTS
(To distinguish between applicants who have met all essential requirements).

Educational/Vocational Qualifications
(Considered to be useful in carrying out the responsibilities of the position)

1. Cisco certifications or equivalent related to network / firewall technologies.
2. ITIL Foundations or Manager V3 / V4 is desirable
3. Formal training and certifications related to Enterprise Storage, Enterprise Backup, Enterprise Virtualisation. Commvault, Hyper-V, VMware highly regarded.

Personal Abilities/Aptitudes/Skills
(Related to the job description and expressed in a way which allows assessment)

1. Proven ability to acquire and maintain knowledge of relevant IT products and methods of IT support delivery.

Experience (Including community experience)

1. Demonstrated experience in designing, planning and migrating on premise networking workloads to cloud environments.
2. Proven experience in management and operation of networking in cloud-based environments.
3. Experience in implementing security controls and policies in an enterprise environment.
4. Experience with the investigation and management of cyber security threats, breaches and security incidents.
5. Demonstrated experience in one or more of the following
    a. Management and configuration of 802.1x environments
    b. Management and configuration of ISE
    c. Experience in support of IPS / IDS environments
    d. Management of PKI infrastructure
    e. Identity and Access Management (IAM)
    f. Azure or other cloud-based infrastructure
    g. SAN networking design, implementation and management / operation including fibre channel networks and switches.
6. Experience in administering complex server environments, including physical, virtual and cloud, in both distributed and central locations. (Hyper-V, VMware or other enterprise virtualisation platforms, Windows operating systems, Active Directory, storage, backup, mail)
7. Experience in operational support and use of Enterprise Email, Enterprise cloud based environments (policies, security, directory), configuration deployment, SIEM, ensuring secure access from public and private environments.

Knowledge

1. Demonstrated knowledge of any of the following
    a. Management, configuration, and support of 802.1x authentication systems
    b. ACSC Essential Eight Maturity Model strategies
    c. South Australian Government Cyber Security Framework (SACSF)
    d. Protective Security Management Framework (PSMF)
    e. ISO27001 and ISO31000 standards
    f. information security governance, risk management, compliance and information security management systems.

2. Knowledge of Public Service Administrative procedures, particularly in relation to the acquisition of information technology related goods, services, and audit requirements.
3. Knowledge of legislation, policies and procedures, including Code of Conduct, EEO and cultural inclusion.

Acknowledged by Applicant..... ...../...../.....