ASO8 Senior Technical Security Specialist
Information Security and Technology Service

ORGANISATIONAL OVERVIEW

South Australia Police (SAPOL) provides a diverse range of services to the community. These services are aimed at producing a safe and peaceful environment by the minimisation of crime and disorder. It is a large complex organisation which, because of the nature of its operations, is constantly subject to public scrutiny and accountability. It provides services to a range of different locations (over 100) spread across the State on a 24 hour a day basis.

SAPOL's vision is to provide 'Safer Communities'. All SAPOL employees are guided by Our Values of Service, Integrity, Courage, Leadership, Collaboration and Respect. SAPOL is an organisation with a proud history and an exciting vision for the future.

POSITION OVERVIEW

Summary

The IS&T Service is responsible for the provision of IT and communications services and is therefore vital to the achievement of SAPOL's core objectives. In consultation with its customers, IS&T plans, develops and implements new and supports existing services. These products and services are provided to agreed quality and service levels.

The Senior Technical Security Specialist, IS&T is accountable to the Manager, IS&T Security for providing management of critical IS&T security functions within the agency.

The role includes:

- Effectively coordinating the day-to-day delivery of Security services provided by a small team of technical staff.
- Closely managing major incidents and issues, driving problem management to identify and remove root cause to prevent reoccurrence and future issues in areas of assigned responsibility.

- Providing professional ICT security-related expertise in a security consulting, advisory, analysis, and facilitating role.
- Providing technical security leadership as an information security subject matter expert.
- Contributing to the risk management of SAPOL information assets by performing threat and risk assessments (TRA) and project risk assessments.
- Performing risk assessments on IS&T systems and providing guidance on security controls for risk treatment; Information Security Management System (ISMS) asset classification, risk definition, and undertaking remedial actions for ongoing management of residual risk and treatments in an ISMS.

Special Conditions

Work Status	The incumbent must hold a current Australian work eligibility status and will be subject to a criminal history check. The incumbent may be assigned to other duties at this remuneration level or equivalent.
Location	Adelaide CBD
Qualifications	N/A.
Out of Hours Work	Some out of hours work may be required.
Travel	Some intrastate and interstate travel may be required.
Performance Management	The incumbent is required to participate in SAPOL's iEngage program.

Reporting / Working Relationships

The Senior Technical Security Specialist:

- Reports to the Manager, Security Architecture and Engineering.
- Coordinates and supports a team of Technical Security Specialists and Security Officers.
- Works closely with managers of the other Branches in IS&T, system owners and users throughout SAPOL, as well as security staff in other agencies and jurisdictions.
- Contributes significantly within a small team of technical staff, supported by external contract resources (e.g. specialist IT security consultants, developers of security solutions), and whole-of-SA Government service providers.
- Works with the agency recognised positions of Agency Security Executive (ASE), Agency Security Advisor (ASA), and Information Technology Security Advisor (ITSA).
- Is a contact point for the South Australian Government Office of Cyber Security and the Cyber Security Watchdesk.

KEY OUTCOMES

Contribute to the Branch decision making, business planning, policy development, service delivery and performance monitoring by:

- Undertaking the business and security analysis of IS&T security related matters and functions including requirements gathering, process mapping and continuous improvement design.
- Developing, implementing and reviewing security policies, standards and procedures for the IS&T Service, ensuring the inclusion of feedback gained by representing SAPOL on external security committees, and contributing to IS&T operational and strategic planning and decision-making.
- Identifying risk exposures by monitoring general system security, access and change control procedures.
- Driving an efficient and consistent approach to access control across SAPOL by developing, documentation, procedures, access control audit reports and general advice.
- Maintaining a knowledge repository of security related information and documents relating to architecture, topology, policies and standards.
- Supporting the induction, training and mentoring of other Security Branch team members.
- Leading the effective management and provision of security services to facilitate business solutions that satisfy client's business requirements.
- Supporting enterprise-wide initiatives and programs via the Security Branch Services to Projects.
- Provision of the highest standards of customer service to clients at all levels by modelling service excellence and by establishing and monitoring structures, systems and standards to achieve high levels of client satisfaction.
- Timely and effective communication to relevant stakeholders on the on-going operation of security services, incident management and Improvement Programmes.
- Ensuring the Branch Business Continuity and Disaster Recovery Plans are always current and actionable.
- Maintaining strong relationships between the Security Branch and internal customers specifically in regard to technology operational services, issues and support.
- Leading the diagnosis of major incidents and issues, identifying and advising on how to remove root causes, preventing reoccurrence and future issues.
- Defining and reporting on a SLA for Security Services throughout SAPOL.
- Contributing to the tactical, resource and strategic planning for the branch, continuous improvement of services provided by IS&T by production incident reporting, identifying and recommending improvements to current solutions, documentation and outcomes.
- Operating under broad guidelines to initiate, plan, implement and deliver significant IT projects as an IT specialist in a multifaceted and complex environment.
- Ensuring a Security Branch on call rotation provides support outside of core business hours for major incidents and high impacting issues.

QUALIFICATIONS / SKILLS / KNOWLEDGE / EXPERIENCE

Essential Minimum Requirements

- Expert knowledge of current IT security technical controls and solutions through the application of risk management techniques to design, deploy and operate security solutions including a demonstrated knowledge of ISO standards and / or the South Australian Government ISMF.

- Ability to develop, implement, manage and evaluate complex security plans, policies, standards and strategies enabling SAPOL to safely and effectively conduct business and achieve its objectives.
- Demonstrated expert technical knowledge and experience in Enterprise Security Architecture, security solution design including the preparation of the following: security business requirements, security high level designs, security low level designs and other security architectural artefacts.
- Demonstrated expert technical knowledge and experience in design, deployment and operational administration, security controls, security configurations, device hardening and security auditing in the following technologies: Windows Server, AD containers/objects including user, groups and service accounts, AD RBAC, MS Certificate Services (PKI), and application internal RBAC.
- Experience in the implementation of Identity Access Management to support role-based access provisioning.
- Demonstrated advanced knowledge of TCP/IP networks, network security, network management and monitoring systems.
- An understanding of the concepts of next generation firewall, virtual private networking, web application firewall, intrusion prevention, endpoint and malicious content management, digital certificates / PKI, authentication protocols and Security Information and Event Management (SIEM).
- Proven ability to effectively coordinate and support a team of professionals providing 1st level Security support in a complex and technical environment, ensuring SLA's are in place and monitored in an environment of continuous improvement.

Desirable Characteristics

- Proven experience in driving the continual improvement of work procedures, policies and practices to meet the business security goals of an organisation.

CORPORATE RESPONSIBILITIES

- Maintain accurate and complete records in accordance with the *State Records Act 1997* and departmental policies, procedures and practice guidance.
- Act at all times in accordance with the Code of Ethics for the South Australian Public Sector and legislative requirements including (but not limited to) the *Public Sector Act 2009* and *Work Health and Safety Act 2012.*
- Actively contribute to SAPOL's commitment to being an inclusive workplace where everyone is safe, respected and supported to reach their potential by demonstrating inclusive behaviour and showing respect for diverse backgrounds, experiences and perspective.
- Demonstrate an understanding and commitment to **WH&S legislation**, principles and practices and risk assessment in accordance with the **WH&S Act (2012)**, regulations, approved codes of practice and AS/NZS ISO 31000:2018 Risk Management – Guidelines.