ASO8 Senior Technical Security Specialist (Prisma Access)
Mobility Transformation Portfolio
Program Delivery
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 Information Systems and Technology (IS&T) Service supports the frontline policing and corporate operations of SAPOL through the provision of ICT infrastructure and communication platforms, operational software applications, and support services. The Service is responsible for driving the ongoing evolution of ICT capability across SAPOL, through the delivery of high-quality ICT change programs. The Service is structured across four core pillars: Strategy, Innovation and Engagement; Program Delivery; Operational Services; and Security and Assurance. The Service extends from traditional ICT services to encompass a specialist radio and technology capability, including laser and radar calibration services.

Program Delivery is accountable for the successful delivery of business outcomes from a large portfolio of projects. It contains both project delivery accountability as well as portfolio governance responsibilities to manage quality, risk and budget to optimise outcomes from the portfolio as a whole. SAPOL is undertaking a large complex portfolio of work across a range

of areas including core infrastructure, business systems and digital transformation initiatives. This full portfolio has been broken into three sub-portfolios to deliver on the business outcomes.

The Mobility Transformation Portfolio is responsible for delivering two flagship programs: the Mobile Workforce Program (MWP), which provides personally issued mobile devices equipped with full frontline capability and the Digital Workforce Program (DWP), which drives digital innovation across SAPOL. Together, these programs form a multi-year, enterprise-wide technology transformation initiative that will shape SAPOL's future workplace and enable next-generation policing through modern, integrated IT solutions.

The Senior Technical Security Specialist (Prisma Access) is accountable to the Program Manager, Mobile Workforce Program for providing management of critical IS&T Prisma Access security functions within the agency.

This position serves as the Senior Technical Security Specialist for Prisma Access within the Mobility Transformation Portfolio, providing day-to-day technical leadership, platform support and continuous improvement of security capabilities. The role oversees the delivery of security services by a small technical team, manages major incidents and drives problem management to address root causes. It delivers specialist ICT security advice and consultancy, acts as an information security subject matter expert and undertakes threat and risk assessments to protect SAPOL information assets. The position also performs security risk assessments on IS&T systems, advises on appropriate security controls and supports ongoing Information Security Management System (ISMS) activities such as asset classification, risk definition and the management of residual risk and treatments.

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 (Prisma Access) reports to the Program Manager, Mobile Workforce Program and serves as the subject matter expert for Prisma Access within the Mobile Workforce Program.

The Senior Technical Security Specialist (Prisma Access) works closely with IS&T managers, system owners and users throughout SAPOL as well as security staff in other agencies and jurisdictions. The position also works as the agency recognised position of Agency Security Executive (ASE), Agency Security Advisor (ASA) and Information Technology Security Advisor (ITSA) and is a point of contact for the South Australian Government Office of Cyber Security and the Cyber Security Watchdesk.

KEY OUTCOMES

- Conducting business and security analysis for Prisma Access, including requirements gathering, process mapping and ongoing improvement of remote access and cloud-delivered security services.
- Develop, implement and review policies, standards and procedures for Prisma Access and cloud-delivered network security, ensuring alignment with ISMF, whole-of-government directives and SAPOL strategic/operational planning input.
- Identify and manage Prisma Access-specific risk exposures by monitoring policy, identity, access and change control activities, ensuring strong configuration governance.
- Driving a consistent and efficient approach to access control and identity integration for Prisma Access (e.g. Azure AD, MFA), supported by robust documentation, audit reports and guidance.
- Maintain a comprehensive and accurate knowledge repository for Prisma Access, including architecture, topology, integrations, policies and standards.
- Induct, train and mentor Security Branch team members in Prisma Access operations, troubleshooting and best practice methods.
- Manage and ensure effective delivery of Prisma Access services that meet business requirements and user experience expectations.
- Provide Prisma Access subject matter expertise to enterprise-wide initiatives and projects, supporting secure-by-design outcomes.
- Deliver high quality customer service and stakeholder engagement for Prisma Access, ensuring clear communication on service status, incidents, changes and improvement initiatives.
- Ensure Prisma Access resilience and service assurance, including current and tested BCDR arrangements, strong vendor and stakeholder relationships, robust incident/problem management, defined SLA's/KPI's, planned upgrades/features under change governance and appropriate on-call support for high-impact incidents.

QUALIFICATIONS / SKILLS / KNOWLEDGE / EXPERIENCE

Essential Minimum Requirements

- Expert technical knowledge and hands on experience with Palo Alto Networks Prisma Access (or equivalent cloud-delivered security platforms), including design, deployment, policy management, troubleshooting and operational administration 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 for cloud-delivered network security, ensuring Prisma Access aligns with enabling SAPOL's security objectives and ISMF. to safely and effectively conduct business and achieve its objectives.
- Demonstrated expert technical knowledge and experience producing security artefacts (requirements, HLD/LLD, runbooks) for Prisma Access and related integrations. 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.

- Advanced knowledge of identity integration and authentication for Prisma Access (e.g. SAML/OIDC/MFA, certificate management/PKI) and of GlobalProtect, routing and traffic steering. 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 implementing and managing ation of Identity and Access Management patterns for Zero Trust Network Access. to support role-based access provisioning.
- Demonstrated advanced knowledge of TCP/IP, routing and networks, network security as applied to cloud-delivered security services and remote access. network management and monitoring systems.
- Strong understanding of next-generation firewall concepts, of next generation firewall, secure web gateway, IPS/IDS, VPN/remote access and SIEM integration, with practical experience integrating Prisma Access telemetry into SIEM for monitoring and threat detection. 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 coordinate internal staff and vendor-managed services to meet SLA's and drive continuous service improvement for Prisma Access. 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.
- Knowledge of Checkpoint firewalls.

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.