Job and Person Specification

Title of Role: Senior Cyber Security Specialist

Remuneration Level: ASO7

Business Unit: Technology Services

Type of Appointment: Term

Division: Projects and Technology

Position Number: P57306

Job and Person Specification Approval

…….. ……../……../…….. Last Reviewed: ……../……../……..

CHIEF EXECUTIVE/DELEGATE

Primary Purpose

The Senior Cyber Security Specialist is responsible for supporting the successful implementation of the Cyber Security and Risk program for the Attorney-General's Department (AGD). The role includes providing professional security-related expertise in a security consulting, advisory, analysis and facilitating capacity, it provides technical security leadership as an information security subject matter expert (SME), contributes to the risk management for information assets by performing threat and risk assessments for various platforms and applications, as well as providing guidance on security controls for risk treatment.

The Senior Cyber Security Specialist works closely with managers of other business areas, systems owners and users throughout AGD. Provides support to the Information Technology Security Advisor (ITSA), as the Deputy ITSA.

Reporting Relationships

- Reports to the Manager, Cyber Security and Risk

Key Relationships/Interactions

- Technology Services
- Projects and Information Technology Teams
- The ICT Security Committee and Agency Security Executive
- Executives and employees across the AGD
- Other Government agencies
- External ICT providers

Key Challenges

- Ability to manage workloads, prioritise tasks and respond at short notice during cyber security events and incidents
- Create collaborative relationships with other members Technology Services, and with key business unit personnel.

Special Conditions

- Some out of hours work may be required
- Occasional interstate and intrastate travel may be required.

AGD Conditions

- Participation in annual performance review and development.
- Actively participate in all mandatory training requirements.
- Abide by the standards in the Code of Ethics for the South Australian Public Sector (the Code).
- Employment is dependent upon a National Police Certificate clearance that the AGD finds satisfactory and a Security Clearance at Negative Vetting Level 1.
- This role is subject to Periodic Criminal History and other Background Screening. The incumbent must participate in criminal history (Police Records Checks) on a periodic basis and be eligible to obtain an Australian Government Security Clearance to the level of Secret (Negative Vetting 1/Baseline).

Flexible Working Arrangement Options

- Flexitime arrangements are available in this role.

Responsibilities

This Job and Person Specification provides an indication of the type of duties you will be engaged to perform. You may be lawfully directed to perform any duties that a person with your qualifications, skills and abilities would reasonably be expected to perform.
The Senior Risk and Cyber Security Specialist is responsible for:

Key Responsibilities	Specified Duties	Performance Indicator/Measurement
Cyber Security and Risk Management	• Develop business cases, and consult on and implement policies in support of the Cyber Security and Risk Program with particular emphasis on the requirements of the ISMF and 'Top 10'. • Provide expert advice on existing and emerging cyber security trends and threats impacting business operations. • Design and implement appropriate security controls to effectively manage risk. • Lead projects for the implementation and ongoing management of event logging and monitoring, and threat and vulnerability management. • Lead the response to incidents of a cyber-security nature. • Develop and lead assurance activities in relation to the requirements of the ISMF and 'Top 10'. • Coordinate with technology and business groups to assess, implement and monitor IT-related security risks/threats. • Perform risk assessments of existing and new services and technologies; communicate findings to risk owners and provide advice that enables informed risk management decisions. • Provide expert advice on governance frameworks, legislation and policies. • Undertake the management of policies, standard, procedures and guidelines throughout the entire lifecycle; undertake breach investigation and lead exemption management. • Participate in governance forums and groups within AGD and externally.	• Controls are in place for identified cyber security risks. • Business units are informed and aware of cyber security risks and controls. • Security initiatives meet whole of government requirements and support AGD strategic objectives. • Compliance with whole of government standards for AGD.
Technical Advice	• Provide expert and specialist advice to stakeholders on matters of cyber security. • Research and propose innovative security solutions, while ensuring minimal end user impact.	• Responsive and accurate technical advice and information is delivered to promote continuous improvement.

Project management and Implementation	• Manage all aspects of specified projects including initiation, development, implementation and evaluation. • Take responsibility for project progress, issues and outcomes, communicating to management in a timely manner. • Initiate and manage actions to rectify variations from agreed project plans. • Proactively manage project scope to ensure successful project delivery. • Lead risk management processes. • Present written and oral briefings to senior management. • Develop and manage project budgets and expenditure. • Manage contracts with suppliers to achieve key performance indicators and agreed targets.	• Projects completed on time and within approved budgets. • Projects implemented according to AGD policy and frameworks. • Risks and issues identified and managed for projects in accordance with policy and process. • Appropriate project documentation developed and maintained throughout projects. • Project plans and reports provided as required. • Budgets developed and managed as required
Communication and Relationship Building	• Establish and maintain open and effective working relationships with management and stakeholders to ensure initiatives are coordinated and milestones are achieved. • Manage stakeholder expectations.	• Stakeholders consulted where appropriate with regard to delivery of outcomes.
Compliance	• Responsible and accountable for adhering to the requirements of the WHS Act 2012; relevant WHS Regulations 2012; the Equal Opportunity Act 1984; the PS Act 2009; the Code of Ethics for Public Sector employees; the principles of diversity; and the Department's policies and procedures. • Keep accurate and complete records of business activities in accordance with the State Records Act 1997.	• Abides by the Acts, Regulations, Policies and Procedures relevant to employees of the Department. • Documents and correspondence filed according to States Records Act, 1997.

Technical Expertise

Qualifications, Skills, Knowledge and Experience relevant to the role

Technical Expertise **(Essential)**	• Expert knowledge of current security technical controls and solutions through the application of risk management techniques to design, deploy and operate security services to deliver practical business solutions. Demonstrated knowledge of the ISO27001/2 standards and the SA Government's ISMF. • Experience in carrying out risk assessments, identifying potential risk events and documenting the probability of occurrence and business impact. • 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, web application security and Security Information and Event Management (SIEM). • Demonstrated expert technical knowledge and experience in, security controls, security configurations, device hardening and security auditing in the following technologies: Windows Server, AD containers/objects including user (privileged and standard), groups and service accounts, AD RBAC, MS Certificate Services (PKI), Application Whitelisting, Application internal RBAC, OS and application patching and security controls (generally). • Demonstrated knowledge of Active Directory (AD) and open systems, TCP/IP networks, network security, network management and monitoring systems, Identity and Access Management (IAM) and cloud security. • Experience in managing authorised penetration tests, technical vulnerability assessments and security audits. • Demonstrated ability to work effectively and with integrity in a high pressure environment. • Excellent interpersonal skills including negotiation, consultation and the ability to influence and gain cooperation. • Highly developed written and verbal communication skills in particular the demonstrated ability to provide sound advice and prepare written reports and briefings to senior stakeholders. • Demonstrated ability to effectively contribute to the management of incidents of a cyber security nature. • Demonstrated ability to successfully manage competing priorities, multiple stakeholders, unplanned change and tight timeframes.
Qualifications (Essential)	• Tertiary qualifications in information technology or other relevant field, and / or security accreditation such as CompTIA Security+, CSX Practitioner, CISSP, CISM or similar.
Technical Expertise (Desirable)	• Knowledge of government processes and proven ability to deliver timely, high quality outcomes within government frameworks. • Knowledge of ICT principles and use within a large diverse organisation. • Experience in implementing and managing Security Information and Event Management (SIEM) for effective threat management. • Experience with secure O365 implementation.

Technical Expertise (cont.)

Qualifications, Skills, Knowledge and Experience relevant to the role

Skills Framework for the Information Age **(Essential)**	• **Consultancy**. Takes responsibility for understanding client requirements, collecting data, delivering analysis and problem resolution. Identifies, evaluates and recommends options, implementing if required. Collaborates with, and facilitates stakeholder groups, as part of formal or informal consultancy agreements. Seeks to fully address client needs, enhancing the capabilities and effectiveness of client personnel, by ensuring that proposed solutions are properly understood and appropriately exploited. • **Business Risk Management**: Carries out risk assessment within a defined functional or technical area of business. Uses consistent processes for identifying potential risk events, quantifying and documenting the probability of occurrence and the impact on the business. Refers to domain experts for guidance on specialised areas of risk, such as architecture and environment. Co-ordinates the development of countermeasures and contingency plans. • **Emerging Technology**: Monitors the market to gain knowledge and understanding of currently emerging technologies. Identifies new and emerging hardware and software technologies and products based on own area of expertise, assesses their relevance and potential value to the organisation, contributes to briefings of staff and management. • **Incident Management**: Prioritises and diagnoses incidents according to agreed procedures. Investigates causes of incidents and seeks resolution. Escalates unresolved incidents. Facilitates recovery, following resolution of incidents. Documents and closes resolved incidents according to agreed procedures. • **Information Security**: Provides advice and guidance on security strategies to manage identified risks and ensure adoption and adherence to standards. Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems. Investigates major breaches of security, and recommends appropriate control improvements. Contributes to development of information security policy, standards and guidelines. • **Penetration Testing**: Coordinates and manages planning of penetration tests, within a defined area of business activity. Delivers objectives insights into existence of vulnerabilities, the effectiveness of defences and mitigating controls – both those already in place and those planned for future implementation. Takes responsibility for integrity of testing activities ad coordinates the execution of these activities. Provides authoritative advice and guidance on the planning and execution of vulnerability tests. Defines and communicates the test strategy. Manages all test processes, and contributes to corporate security testing standards. • **Security Administration:** Maintains security administration processes and checks that all requests for support are dealt with according to agreed procedures. Provides guidance in defining access rights and privileges. Investigates security breaches in accordance with established procedures and recommends required actions and supports / follows up to ensure these are implemented. • **Technical Specialism**: Maintains knowledge of specific specialisms, provides detailed advice regarding their application and executes specialised tasks. The specialism can be any area of information or communication technology, technique, method, product or application area.

Behaviour Capabilities

Descriptors below detail the behavioural skills and capabilities required for performance in the Network Specialist. In this table the KEY behaviours for this role have been selected from the larger number of relevant behaviours for each element AGD's Performance Matrix. This broader group of behaviours are applicable to your success in this role. **Behaviours critical to the role are highlighted in bold.**

Elements	Behaviours
Promotes Strategic Thinking and Change	• Translates strategies and goals into achievable plans • Ensures work goals are linked to the bigger picture • **Adopts and manages a balanced approach to risk aversion and risk taking** • Drives effective change • **Promotes creative and innovative thinking**
Achieves Team Results	• Provides clear direction on how to achieve outcomes • **Develops plans with clear outcomes and supports others to achieve these** • Confidently makes decisions showing good judgement • **Effectively prioritises and re-negotiates tasks as needed** • Reviews performance and seeks opportunities to implement continuous improvement
Delivers Business Excellence	• **Identifies trends, potential problems and opportunities and incorporates into plans** • **Effectively manages and coordinates resources for optimal outcomes.** • Promotes a culture of financial responsibility, accountability and awareness • **Sets clear performance standards that are linked to business unit outcomes.**
Establish Relationships and Engages Others	• Represents the agency and public sector effectively in public and government forums • Develops effective working relationships and internal and external networks • **Appropriately identifies and collaborates with relevant stakeholders** • **Shares information and knowledge** • **Tailors approach and communication style to suit the situation and audience** •
Promotes Personal Drive and Professionalism	• Builds a culture of respect and high ethical standards • **Demonstrates and promotes professionalism and confidentiality when dealing with sensitive issues** • **Willing to put own views forward and challenges opposing views in a respectful manner** • Promotes a high standard of wellbeing for self and others

Acknowledged by occupant	_____ (Print name)	_____ (Signature)	/ / _____
Acknowledged by line manager	_____ (Print name)	_____ (Signature & title)	/ / _____

•