# Job and Person Specification

| | | | |
|---|---|---|---|
| **Title of Role:** | Cyber Security Architect | **Remuneration Level:** | ASO8 |
| **Business Unit:** | Technology Services | **Type of Appointment:** | Ongoing |
| **Division:** | Projects and Technology | **Position Number:** | P68110 |

**Job and Person Specification Approval**

……..…../……../…….. DELEGATE

## Primary Purpose

The Cyber Security Architect provides authoritative leadership and specialist expertise to define, embed and assure cyber security requirements across departmental operations. The role is responsible for translating cyber security strategy, standards and governance into effective architectural patterns, security controls and operational practices that protect information assets and enable secure service delivery. Operating with a high degree of autonomy, the role influences solution design, risk management and assurance activities to ensure cyber security obligations are consistently met and sustained across the department.

## Job Environment

The Cyber Security Architect operates within the Cyber Security team, part of Technology Services, in a complex and evolving technology and threat environment. The role functions at a senior specialist level and contributes to department-wide cyber security outcomes that support secure service delivery, information protection and regulatory compliance.

## Reporting Relationships

Reports to Manager, Cyber Security and Risk

## Key Relationships/Interactions

- Cyber Security
- Architecture
- Project Management Office
- AGD Executives and stakeholders

## Key Challenges

- Operating with a high level of autonomy and accountability
- Influencing senior stakeholders and organisational direction
- Balancing security, risk, and business enablement
- Driving capability uplift and continuous improvement
- Navigating complex regulatory and compliance requirements
- Working within a diverse organisation with competing priorities

## AGD Conditions

- Effectively embed AGD People and Leadership Expectations into all actions, activities and work processes
- Participate in bi-annual Performance Development Plan (PDP)
- Proactively seek learning opportunities, including in the timely completion of all mandatory training requirements
- Comply with the Code of Ethics for the South Australian Public Sector, relevant legislation and AGD policies and procedures
- Employment is dependent upon a compliant National Police Certificate that the AGD finds satisfactory.
- This role requires the incumbent to obtain:
    - Working with Children Check
    - AGSVA Security Clearance (Baseline)

## Diversity

The Attorney-General's Department values workplace diversity and is committed to providing an inclusive work environment where employees feel respected, valued and empowered to be themselves, we are also committed to reconciliation and strongly value First Nation's perspectives in the community and workplace.

## Flexible Working Arrangement Options

The South Australian public sector promotes diversity and flexible ways of working including part-time. You are encouraged to discuss the flexible working arrangements for this role. Flexible working arrangement options for this role may include:

- Flexitime
- Part-time
- Job Sharing
- Compressed weeks
- Work from home arrangements

## 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 Cyber Security Architect is responsible for:

| Key Responsibilities | Specified Duties | Performance Indicator/Measurement |
|---|---|---|
| **Cyber Security Strategy and Architecture** | • Define, maintain and evolve departmental cyber security architecture, principles and patterns to support the implementation of the cyber security strategy and delivery of service catalogue.<br>• Provide authoritative advice on emerging threats, architectural risks and control maturity to inform strategic decision-making.<br>• Review and guide solution architectures, system designs and development initiatives to ensure cyber security requirements are embedded by design and by default.<br>• Assess proposed technologies and solutions for security risks, control adequacy and compliance with relevant frameworks and standards.<br>• Provide architectural direction and recommendations to project teams, solution architects and technical specialists. | • Cyber security architecture artefacts (principles, standards, reference architectures) are current, approved, and demonstrably aligned to departmental and whole-of-government strategy.<br>• Security architecture decisions consistently enable secure business outcomes while balancing risk, cost and operational impact.<br>• Strategic cyber security advice is sought by senior stakeholders and influences departmental |

| Key Responsibilities | Specified Duties | Performance Indicator/Measurement |
|---|---|---|
| | | planning and investment decisions. |
| **Solution Architecture Assurance** | • Review and guide solution architectures, system designs and development initiatives to ensure cyber security requirements are embedded by design and by default.<br>• Assess proposed technologies and solutions for security risks, control adequacy and compliance with relevant frameworks and standards.<br>• Provide architectural direction and recommendations to project teams, solution architects and technical specialists. | • Security requirements are embedded early in solution design and development, reducing the need for late-stage remediation.<br>• Architectural reviews identify material security risks and result in practical, risk-based recommendations that are adopted by delivery teams.<br>• Approved solutions demonstrably meet defined cyber security requirements and standards prior to production deployment.<br>• Stakeholders report clarity and value in security architecture guidance provided to projects and programs. |
| **Cyber Security Governance** | • Define, support and continuously improve cyber security governance arrangements, including policies, standards, guidelines and architectural artefacts.<br>• Contribute to governance forums and provide expert input to support informed risk acceptance and control decisions.<br>• Contribute to assurance activities, reviews and audits by providing architectural evidence, expert analysis and remediation guidance.<br>• Support continuous improvement of security controls and assurance outcomes. | • Cyber security policies, standards and guidelines are clear, fit-for-purpose, and consistently applied across Technology Services.<br>• Governance artefacts are maintained and reviewed in line with business, technology and threat landscape changes. |
| **Cyber Security Risk Management** | • Support cyber security risk identification, assessment, treatment and monitoring across departmental systems and services.<br>• Ensure security architecture decisions are informed by risk and aligned with the department's risk appetite.<br>• Provide specialist advice on risk mitigation strategies and residual risk management. | • Cyber security risks are clearly articulated, assessed and prioritised in accordance with departmental risk management practices.<br>• Architectural and control recommendations demonstrably reduce risk or align residual risk with the department's risk appetite.<br>• Risk treatment strategies are pragmatic, cost-effective |

| Key Responsibilities | Specified Duties | Performance Indicator/Measurement |
|---|---|---|
| | | and supported by evidence.<br>• Senior stakeholders are appropriately informed of cyber security risk implications and options. |
| **Leadership and Capability Development** | • Provide leadership and mentoring to members of the cyber security team and broader technology community.<br>• Influence stakeholders across Technology Services and the business to uplift cyber security maturity and architectural discipline.<br>• Promote a culture of security-by-design and shared accountability for cyber security outcomes | • Cyber security team members receive clear architectural direction, mentoring and professional guidance.<br>• Capability uplift is evident through improved consistency, quality and confidence in security-by-design practices.<br>• The role positively influences cyber security culture across the department.<br>• Collaboration with peers and stakeholders strengthens whole-of-team and cross-functional outcomes. |
| **Contribute to Culture** | • Display constructive behaviours in line with AGD's people expectations of self-awareness, building trust, and building teams.<br>• Seek feedback and review personal performance.<br>• Develop effective working relationships, be approachable and work cooperatively with others to achieve outcomes.<br>• Communicate proactively and prioritise workload effectively, asking for guidance and negotiating deadlines where appropriate.<br>• Identify and undertake personal professional development.<br>• Actively participate and contribute to responsible and safe work practices.<br>• Embrace diversity and cultural differences in the workplace. | • Feedback on performance from peers and leaders is positive.<br>• Priorities are effectively communicated and negotiated.<br>• Personal development is undertaken.<br>• Work practices are safe and Work Health and Safety legislation, policies and procedures are adhered.<br>• Respectful behaviour observed when faced with diversity/differences in opinion. |

## Capabilities relevant to the role (Qualifications, Skills, Knowledge and Experience)

| | |
|---|---|
| **Essential** | • Significant demonstrated experience and expertise in strategic planning, cyber security, and security architecture in a large enterprise ICT environment.<br>• Demonstrated strong understanding of cyber security standards, architectural frameworks and technologies. |

| | |
|---|---|
| | • Demonstrated technical experience across a wide variety of technologies including cloud, network, applications and platforms.<br>• Demonstrated experience in system security threat analysis and risk assessments, policy and standard development, architecture and design.<br>• Demonstrated ability to contribute to a constructive workplace culture.<br>• High level interpersonal skills and ability to establish and maintain productive working relationships with colleagues and other relevant stakeholders. |
| **Desirable** | • Strong working knowledge of, and ability to apply:<br>  • South Australian Cyber Security Framework (SACSF)<br>  • ISO/IEC 27001 – Information Security Management Systems<br>  • ISO/IEC 27002 – Information Security Controls<br>• Tertiary education or industry certification such as:<br>  • CISSP (Certified Information Systems Security Professional)<br>  • CCSP (Certified Cloud Security Professional)<br>  • SABSA Chartered Security Architect/TOGAF<br>  • Vendor-specific training such as Microsoft SC-100, AWS Certified Security - Specialty |

## Behavioural Capabilities and AGD People Expectations

The AGD Performance Matrix describes the behaviours expected of AGD employees across various levels in the Department. All employees are expected to behave in accordance with the AGD People Expectations of being self-aware, building trust and building teams. Descriptors below detail the behavioural capabilities required for performance in the Cyber Security Architect. KEY behaviours for this role are listed with the critical behaviours highlighted in **bold**. This broader group of behaviours are applicable to your ongoing success in the role.

| | **Strategic Focus** | **Results Orientation** | **Service Delivery Excellence** | **Relationship Management** | **Professional Approach and Drive** |
|---|---|---|---|---|---|
| **Strategic** | Shapes Strategic Thinking and Change | Achieves Organisational Results | Drives Business Excellence | Forges Relationships and Engages Others | Exemplifies Personal Drive and Professionalism |
| **Tactical** | **Promotes Strategic Thinking and Change** | **Achieves Team Results** | **Delivers Business Excellence** | **Establish Relationships and Engages Others** | **Models Personal Drive and Professionalism** |
| **Operational** | Supports Strategic Direction | Achieves and Monitors Own Results | Supports Service Delivery Excellence | Fosters Working Relationships | Supports Personal Drive and Professionalism |
| **Foundational** | Understands the Strategic Direction | Achieves Individual Results | Contributes to Service Delivery Excellence | Maintains Working Relationships | Demonstrates Personal Drive and Professionalism |

| Element | Behaviours |
|---|---|
| **Promotes Strategic Thinking and Change** | • Actively promotes goals and strategic direction<br>• **Translates strategies and goals into achievable plans**<br>• Ensures work goals are linked to the bigger picture<br>• **Adopts and manages a balanced approach to risk aversion and risk taking**<br>• Considers the broader political environment and context when decision making<br>• Sets aside time to engage in forward planning for his/her area of responsibility<br>• Drives effective change<br>• Promotes creative and innovative thinking |
| **Achieves Organisational Results** | • Brings together concepts and ideas into clear strategies and translates them into concrete implementation plans<br>• **Holds self and others accountable for quality, timely and cost-effective results**<br>• **Makes complex decisions that require a high degree of judgement**<br>• Monitors performance and drives continuous improvement |

| | |
|---|---|
| **Delivers Business Excellence** | • Identifies trends, potential problems and opportunities and incorporates into plans<br>• **Promotes and ensures a strong focus on internal and external customer service**<br>• Sets clear performance standards that are linked to business unit<br>• outcomes.<br>• Effectively manages their own, individual and team performance and<br>• contribute to the business unit<br>• Provides clear, honest and timely feedback, including addressing non-performance promptly and recognising high performance. |
| **Establish Relationships and Engages Others** | • Represents the agency and public sector effectively in public and government forums<br>• Develops effective working relationships and internal and external networks<br>• **Appropriately identifies and collaborates with relevant stakeholders**<br>• Shares information and knowledge<br>• **Tailors approach and communication style to suit the situation and audience**<br>• Identifies opportunities to negotiate for improved outcomes<br>• Actively listens and communicates in a clear and concise manner |
| **Models Personal Drive and Professionalism** | • Builds a culture of respect and high ethical standards<br>• Promotes diversity and uses this to enhance outcomes<br>• Demonstrates and promotes professionalism and confidentiality when dealing with sensitive issues<br>• Willing to put own views forward and challenges opposing views in a respectful manner<br>• **Identifies and considers risk in decision making**<br>• Remains positive and recovers quickly from setbacks<br>• **Promotes adaptability in dealing with change**<br>• Seeks opportunities to strengthen areas for development<br>• Seeks feedback on performance and engages in self-reflection<br>• Promotes a high standard of wellbeing for self and others |

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