JOB AND PERSON SPECIFICATIONS

Position Title:	**Cyber Security Program Manager**
Position No:	**TBC**
Classification Level:	**ASO7**
Type of Appointment:	**Temporary term up to 18 December 2026**
Branch:	**ICT**
Date Updated:	**June 2025**

JOB SPECIFICATION

ROLE SUMMARY

The Cyber Security Program Manager is responsible for the development and implementation of a Cyber Security Program for the 2026 state, first nations voice to parliament and local council elections. This will include the coordination of key activities to support compliance with the South Australian Cyber Security Framework (SACSF) and South Australian Protective Security Framework (SAPSF) and Information Security Policies.

The role will provide professional security-related expertise in a security consulting, advisory, analysis and facilitating capacity, along with technical security leadership as an information security subject matter expert, and support the Information Technology Security Advisor (ITSA) and Agency Security Executive (ASE).

The Cyber Security Program Manager will report to the Manager ICT, will work closely with internal and external stakeholders (government and non-government), as required.

KEY RESPONSIBILITIES

- Develop business cases, consult on and implement policies to support the Cyber Security Program with emphasis on the SACSF and Guidelines and Information Security Policies under the SAPSF.
- Provide expert and specialist advice to the Electoral Commissioner, Deputy Electoral Commissioner, ITSA and other stakeholders on matters of cyber security.
- Provide expert advice on existing and emerging cyber security trends and threats impacting business operations, and specifically election events.
- Design and implement appropriate security controls to effectively manage risk.
- Research and propose innovative security solutions, while ensuring minimal end user impact.
- Lead the implementation and management of event logging and monitoring, and threat and vulnerability management.

- Lead the response to cyber security incidents.
- Develop and lead assurance activities in relation to the requirements of the ISMF.
- Coordinate with the broader ICT team to assess, implement and monitor IT-related security risks and 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.
- Managers contracts with suppliers as required.
- Develop an information registry.
- Develop and implement a dedicated business continuity plan for cyber security incidents.
- Provide high level briefings and reports for the consideration of the executive, relevant oversight committees and groups.
- Participate in program and project governance via PMO review and steering committees as relevant.
- Ensure ECSA applies and maintains compliance with the Government ICT Security Framework and relevant security standards, including the SACSF.
- Proactively identify opportunities for, and foster a culture of, continuous improvement.

AGENCY RESPONSIBILITIES

- Contribute to effective election management and the provision of best practice electoral services by investigating opportunities to enhance operations and assuming responsibility for specific state and local government electoral projects and agency projects.
- Demonstrate appropriate and professional workplace behaviours that are in-line with the Code of Ethics for the South Australian Public Sector.
- Maintain a commitment to EEO, Diversity and Ethical Conduct according to the principles of the Public Sector Act 2009.
- Contribute to a safe and healthy work environment by taking reasonable care to protect your own and others' health and safety at work by having a knowledge of, and complying with, legislation and ECSA policies and procedures related to the Work Health and Safety Act 2012 (SA).
- Utilise resources and information in a responsible and accountable manner and comply with all Public Sector and ECSA financial, procurement, IT and HR policies and procedures.
- Actively participate in ECSA's Performance Management and Development Program.
- Uphold the values of ECSA as reflected in the Strategic Plan.
- Adhere to quality service standards to ensure objectives of ECSA's Customer Service Charter are fulfilled.
- Keep accurate and complete records of business activities in accordance with the State Records Act 1997.

You may be lawfully directed to perform any duties that a person with your qualifications, skills and abilities would reasonably be expected to perform.

SPECIAL CONDITIONS

- In order not to compromise the strict neutrality of the Commission, no person who is active in political affairs or intends to carry on this activity may be an employee.
- Employment is dependent upon a National Police Certificate clearance that the Commission finds satisfactory.
- Extensive out of normal working hours duty may be required during the period of an election.
- ECSA staff will be required to work collaboratively with both internal and external staff, contractors, and service providers to ensure smooth operations of ECSA functions, in particular during election events.
- ICT staff will be required to remain current in their training related to technology and data security and understand roles and notification requirements in the event of an incident or breach.
- Some interstate and intrastate travel may be required.
- Incumbent must have or be able to obtain and maintain a security clearance at the Baseline level or above.

PERSON SPECIFICATION

ESSENTIAL REQUIREMENTS

Qualifications

- Tertiary qualifications in information technology or other relevant field, and/ or security accreditation such as CompTIA Security+, CSX Practitioner, CISSP, CISM or similar.

Personal Abilities, Aptitudes, Skills

- Proven ability to work under broad direction and successfully manage multiple concurrent work demands, dealing with competing priorities, multiple stakeholders, unplanned change and meeting immutable deadlines.
- Highly developed written and verbal communication skills with demonstrated ability to provide sound advice and prepare written reports and briefings for senior stakeholders.
- Excellent interpersonal skills including negotiation, consultation and the ability to influence and gain cooperation.
- Proven ability to establish, manage and administer significant projects to achieve successful outcomes.
- Proven ability to effectively contribute to the management of cyber security incidents.
- Demonstrated capacity to work effectively, and exercise sound judgement in a complex and changing environment.
- Display drive, initiative and enthusiasm and the ability to meet tight deadlines.

Experience

- Experience in carrying out risk assessments, identifying potential risk events and documenting the probability of occurrence and business impact.
- 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).
- Experience in managing authorised penetration tests, technical vulnerability assessments and security audits.

Knowledge

- 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 solutions.
- Demonstrated knowledge of ISO27001/2 standards and the SA Government's Information Security Management Framework and Cyber Security Framework.
- 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 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.

DESIRABLE CHARACTERISTICS

Qualifications

- None specified.

Personal Abilities, Aptitudes, Skills

- None specified.

Experience

- Experience in implementing and managing Security Information and Event Management (SIEM) for effective threat management.
- Experience in managing ICT systems for a public sector agency or organisation.

Knowledge

- Knowledge of electoral commissions and electoral processes.
- Knowledge of government processes and proven ability to deliver timely, high quality outcomes within government frameworks.
- Knowledge of ICT principles and use within a complex organisation.

Reviewed and approved by Deputy Electoral Commissioner:			
Accepted by Employee:			/ /
	Name	**Signature**	**Date**