ROLE STATEMENT

ROLE TITLE	Cyber Security Officer	**POSITION NO.**	TBA
CLASSIFICATION	ASO5	**REVIEWED DATE**	September 2026
PORTFOLIO	Experience & Learning	**AGENCY**	History Trust of SA
ANZSCO CODE	261112		

ABOUT THE ROLE

The Cyber Security Officer provides the day-to-day operational coordination, assurance and improvement capability required to protect HTSA information, systems, websites, cloud services, and public-facing digital services. The role translates cyber security policies and risk decisions into practical controls, evidence, remediation activity, staff guidance, and incident readiness.

Reporting to the Manager, Digital, who retains responsibility for cyber security governance, risk management, strategic priorities and SACSF/SAPSF attestation, the Cyber Security Officer works closely with the broader Digital team, managed service providers, application vendors and business system owners.

HTSA operates a broad digital environment spanning Microsoft 365 and identity services, enterprise and museum-specific applications, websites, visitor-facing platforms, museum interactives, endpoint devices, infrastructure and managed services. Cyber security responsibilities currently sit across leadership and technical roles. This position creates a clear operational focal point while retaining control of ownership with the team members who administer the relevant systems.

Reporting/Working Relationships

- Reports to the Manager, Digital
- Works closely with the Digital team
- Works closely with the whole HTSA team

Why Join the History Trust of South Australia?

The History Trust connects people with the stories that shape our state. We put history to work, helping South Australians understand the past and make better decisions about the future. Through our collections, museums, events and education programs, we use history as a training ground for thinking about the impacts of the choices we make. Joining the History Trust means contributing to work that strengthens learning, civic life and community understanding across South Australia.

Benefits of Working with Us

Looking for a role that combines a deeper purpose with your skills? At the History Trust of South Australia, we do things a little differently. We leap at opportunities and create our own, and we practise what we preach by giving people the space to test ideas, learn, and keep improving. We welcome ambition and, most of all, gumption, the resourcefulness, creativity and tenacity needed to get things done. This is a role suited to someone who enjoys variety, initiative, and developing practical solutions. Alongside meaningful work, you will find a collaborative culture and flexible working arrangements where possible.

SECTION A: KEY ACCOUNTABILITIES

- Develop, maintain and implement cyber security standards, procedures, and associated plans and Programs in accordance with approved policies and frameworks.
- Undertake cyber risk assessments, support the development and implementation of risk treatments, contribute to assurance activities, and provide sound advice and recommendations to mitigate security risk.
- Undertake supplier cyber risk assessments and due diligence, support security activities in procurement and contract management activities and provide ongoing assurance reviews and issue resolution of applications.
- Support the practical implementation of cyber security controls and solutions, including secure configuration, operation and assurance of platforms and applications, including documentation and validation activities.
- Analyse vulnerability and threat information, prioritise findings using risk-based approaches, implement and/or coordinate remediation activities, track and monitor progress and escalate overdue or high-risk items.
- Develop and maintain security monitoring use cases and detection to reduce false positives and improve security outcomes.
- Perform incident triage, assessment and classification, coordinate response activities in line with approved incident response plans and escalation procedures.
- Conduct investigation activities to confirm impact and scope, and recommend containment, eradication and recovery actions.
- Promote cyber security awareness and good practice across the History Trust, provide practical guidance to staff, coordinate security training and work with internal teams and external service providers to strengthen organisational cyber security capability.
- Conduct post-incident reviews, document lessons learned and implement and/or coordinate continuous improvement initiatives.

SECTION B: Selection Criteria

TECHNICAL EXPERTISE

Essential:

- Demonstrated experience in cyber security operations, governance, risk, compliance and assurance, with the ability to apply security frameworks and support effective security outcomes across an organisation.
- Practical experience in vulnerability management, incident response, identity and access management, and the implementation of cloud, endpoint and website security controls.
- Experience working with Microsoft 365, Entra ID, Intune, Defender and South Australian Government cyber and protective security requirements, including assurance and compliance activities.
- Proven ability to coordinate security remediation and improvement initiatives across internal stakeholders, service providers and vendors, while supporting security awareness, incident preparedness and continuous improvement.

PERSONAL ABILITIES

- Excellent interpersonal skills; building effective networks and operational relationships with internal and external clients, service providers and stakeholders and a confident and professional approach to dealing with a range of internal and external stakeholders including volunteers and community members.
- Demonstrated ability to communicate effectively, both verbally and in writing, problem solve and establish and maintain effective working relationships with a diverse range of people.

- Demonstrated ability to work under limited direction, either independently or as a member of a team, to identify performance outcomes, determine priorities, plan and organise work and utilise judgement and delegated authority to perform technical tasks to achieve performance outcomes.
- Demonstrated ability to select methods and techniques based on sound judgement, to research, analyse, report and present material appropriate to the audience, and to assess new concepts and resolve technical problems.

EXPERIENCE

- Experience supporting cyber security governance, risk and assurance activities, including maintaining documentation, registers, metrics and reporting.
- Experience developing and applying cyber security policies, procedures, frameworks and controls within a government or regulated environment.
- Experience supporting identity and access management activities, including access provisioning, reviews, compliance monitoring and issue escalation.
- Experience supporting cyber security operations, including vulnerability management, security monitoring, incident response, supplier assurance and remediation activities.

QUALIFICATION

Essential: Nil

Desirable:

- Relevant tertiary qualification or industry certification in cyber security, information technology, cyber risk, cyber audit or related discipline.

SPECIFIC REQUIREMENTS

All employees commit to valuing and respecting the needs and contributions of First Nations employees and visitors, and to developing intercultural capability, including engagement with the Culturally and Linguistically Diverse (CALD) community.

Engagement in this role is subject to a satisfactory Department of Human Services Working with Children Check, with renewal required every five years.

The role may require out-of-hours work, as well as intrastate and interstate travel.

All History Trust of South Australia employees are required to work in accordance with the Code of Ethics for the South Australian Public Sector, as well as relevant policies, procedures, and legislative requirements, including but not limited to:

- Work Health and Safety Act 2012 (SA)
- Return to Work Act 2014 (SA)
- Equal Employment Opportunity (including prevention of bullying, harassment, and intimidation)
- Children's Protection Act 1993 (Cth) – Notification of Abuse or Neglect
- Public Interest Disclosure Act 2018
- Disability Discrimination legislation
- Information Privacy Principles
- Relevant Awards, Enterprise Agreements, Public Sector Act 2009, History Trust of SA Act 1981, and OCPSE Determinations and Guidelines
- Relevant Australian Standards
- Applying the principles of the South Australian Government's Risk Management Policy as appropriate

- Maintaining accurate and complete records of business activities in accordance with the State Records Act 1997

This role is based in the Adelaide CBD, however it is required to regularly travel between our sites located in Birdwood, Port Adelaide, Walkley Heights and Adelaide CBD. Depending on operational needs, the incumbent may be required to transfer to other History Trust locations, either permanently or temporarily, to perform work appropriate to their classification, skills, and capabilities, in accordance with the relevant provisions of the Public Sector Act 2009.

Work Health and Safety

This role requires the incumbent to:

- Lead workplace safety procedures and programs
- Ensure interns and other workers under the role's supervision understand relevant workplace health and safety requirements and responsibilities.
- Lead and participate in health and safety discussions in the workplace.
- Identify hazards, assess risks, and implement procedures for controlling risks.
- Implement procedures for dealing with incidents and emergency events.
- Maintain appropriate workplace safety records.
- Implement procedures for managing injured workers.