South Australian Cyber Security Framework

Government of South Australia

Document Control

ID	SACSF
Version	V1.0
Classification/DLM	OFFICIAL
Compliance	Mandatory
Original authorisation date	November 2019
Last approval date	November 2019
Next review date	November 2020

Licence

Table of contents

1. Foreword

The Government of South Australia manages, delivers and owns a range of information technology infrastructure, services and systems on behalf of the citizens of South Australia. In order to uphold citizen's trust and confidence, and to ensure services delivered to the community are reliable and resilient, it is imperative that government agencies safeguard infrastructure, digital assets and citizen information against cyber threats.

The South Australian Cyber Security Framework (SACSF) is a cabinet approved, whole of government policy framework which draws on international best practice for risk-based cyber security management. While the SACSF applies to all government agencies and their suppliers, it is not a one-size-fits-all or compliance approach to cyber security. Rather the SACSF reinforces the need for cyber security to be an enabler for government and drives this via a risk-based approach. This approach helps ensure risks are managed in a way that is commensurate with the risk appetite of the agency.

The objectives of the SACSF are to:

- Ensure cyber security risks are managed in an acceptable way.
- Provide assurance to the South Australian public and other interested parties that the information entrusted to the State Government is adequately protected.
- Maintain the confidentiality, integrity and availability of information assets in alignment with necessary policy, legal and regulatory requirements.
- Maintain the reputation of the individual agencies and the broader South Australian Government.
- Help embed cyber risk management as part of an agency's existing risk management framework.
- Demonstrate alignment to internationally recognised good practice in cyber risk management.

This approach will help deliver more responsible data sharing for social change, better protect the safety and prosperity of South Australians, and enhance the government's digital engagement with the business community.

2. Introduction

2.1 Background

The South Australian Cyber Security Framework (SACSF) has been developed to standardise and guide the approach for establishing, implementing, maintaining and continually improving the cyber security posture of South Australian Government agencies.

For the purposes of this document cyber security refers to the measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means.

The SACSF is a risk-based framework developed to assist with preserving the confidentiality, integrity and availability of information by applying risk management processes, with increasing control measures to be implemented based on increased likelihood or impact. A risk-based approach to cyber security management provides flexibility for an agency to implement controls based on its own risk profile, as opposed to a one-size-fits-all approach.

The SACSF is supported by a significant suite of supporting documentation, guidance and templates to help an agency implement the framework based on their risk profile and in line with an agency's existing risk management framework.

The SACSF is maintained by the Office for Cyber Security in the Department of the Premier and Cabinet (DPC) and is a subordinate document to the Protective Security Policy Framework.

2.2 Purpose

The SACSF outlines the mandatory requirements to which all SA Government agencies must adhere and as well as a set of supporting expectations. This document is designed to be used by all personnel within an agency including senior leadership, business unit managers, information technology staff, and audit and risk teams.

Relevant sections of the SACSF will also apply to suppliers to SA Government as well as non-government personnel that provide services to government agencies.

2.3 Authority

The SACSF is a Cabinet-approved document that describes 21 policy statements in support of contemporary practices for the security of information stored, processed, transmitted or otherwise manipulated by information and communication technology (ICT).

2.4 Applicability

The SACSF applies to:

- South Australian Government public sector agencies (agencies), that is, administrative units, bodies corporate, statutory authorities, and instrumentalities of the Crown. Refer: Public Sector Act 2009
- Suppliers to the South Australian Government and non-government personnel that provide services to government agencies.

Reliance upon this policy or standard by any other person is entirely at their own risk and the Crown in the right of South Australia disclaims all responsibility or liability to the extent permissible by law for any such reliance.

3. Implementation Approach

This section provides overview of key elements that must be considered as part of the implementation of the SACSF. Each section has underlying guidance and templates that agencies may utilise to assist with implementation of the SACSF.

3.1 Cyber Security Risk Appetite

The agency Chief Executive is required to approve the cyber security risk appetite statement for their agency. This statement defines, at a high level, the appetite that the agency has for cyber security risks.

As a minimum, it is expected that each agency defines their appetite toward cyber security risks that may impact:

- The health and safety of agency personnel and the South Australian community,
- The confidentiality and integrity of information held by the agency,
- The strategic objectives of the agency, and
- The reputation of the agency with key stakeholders

Additional information and guidance:

Cyber Security Risk Appetite Guidance

3.2 SACSF Tier Selection

The SACSF sets out a tiering model to help provide guidance around the security controls and measures that agencies should consider based on the size, complexity and criticality of their agency.

Agency Chief Executives are required to approve a tier level for their agency taking into consideration such factors as:

- The cyber security risk appetite of the agency;
- The classification of information held by the agency;
- The criticality of services provided by the agency;
- The agency's size and resourcing capability; and
- The perceived overall risk of the agency.

The whole of government ICT and Data Board will note each agency's tier selection.

Additional information and guidance:

Appendix C: Guidance on Tier Selection

3.3 The Cyber Security Program

Effective implementation of the SACSF requires the development of a cyber security program (CSP). The CSP work program helps demonstrate an agency's ongoing commitment and approach to managing cyber security risk.

The program of work should take into consideration:

- The strategic cyber security objectives of the agency in alignment with the SACSF,
- The SACSF tier selected by the agency, including selection justification,
- The cyber security risk appetite of the agency,
- The cyber security governance model to be used by the agency including the key cyber security responsibilities of functions within the agency,
- The scope, boundaries and exclusions of the cyber security program,
- The interested parties (i.e. stakeholders) that require the agency to implement robust cyber security controls,
- Applicable legal, regulatory and contractual requirements of the agency.

Additional information and guidance:

Cyber Security Program Template

3.4 The Cyber Security Calendar

A cyber security calendar (may also be referred to as an Information Security Calendar, Information Assurance Calendar or similar) should be developed to support the cyber security work program and track key initiatives and ongoing operational tasks. This

calendar will form a key component of the agency's annual attestation of their current alignment to the SACSF.

Additional information and guidance:

Security Calendar Template

3.5 Asset Identification & Classification

Agencies are to identify and document their critical processes and services, and the information assets used to support these processes. These information assets are to be classified for confidentiality, integrity and availability requirements thereby providing the agency with context for their risk assessment.

Additional information and guidance:

South Australian Information Classification System

SACSF Guideline 6.0 Integrity and Availability Classification using the SACSF Information Asset Register Template

3.6 Risk Assessment

A risk assessment is to be conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of personnel throughout the agency.

Cyber security is founded on risk management. Agencies must manage risk to reduce their likelihood and/or mitigate their business consequences, balancing the cost of security with its outcomes. Absolute security is unaffordable, often unachievable, and may impede business objectives and/or efficiencies.

Agencies are to identify and evaluate their cyber security risks and determine the required risk treatment activities in line with business requirements.

Additional information and guidance:

Risk Register Template

3.7 Framework Implementation Guidance

Each agency will implement controls to meet the requirements of each of the 21 policy statements. In addition to technical and procedural controls, this will include the development and implementation of a suite of approved cyber security artefacts, formalising the implemented controls and associated processes.

Additional information and guidance:

SACSF Implementation Toolkit

SACSF Guideline 3.0 Engaging Suppliers and Cloud Security

Measures and Metrics Guidance

Supplier Security Questionnaire

Supplier Register Template

Cyber Security Policy Template

Cyber Security Employee Handbook Template

Corrective Actions and Improvements Register

3.8 Independent Certification

Agencies are encouraged to consider certification of their Cyber Security Program and Framework to the ISO 27001:2013 Information Security Management Standard. This certification provides independent assurance that the agency is managing cyber security risks, whilst also satisfying a key policy statement of the SACSF (1.6: Audit and Assurance).

3.9 Annual Attestation

Each agency is to provide an annual attestation to the Department of the Premier and Cabinet which details its current state of alignment to the SACSF together with the plan to meet or maintain alignment to the requirements of the agency's selected tier level.

The attestation will be endorsed by the Agency Security Committee, reviewed by Senior Leadership, and approved by the Chief Executive.

At a high level, the attestation will cover:

- Tasks completed during the reporting period,
- Tasks to be completed during the new reporting period,
- Responsibility for completing the associated task, and
- Cyber security program funding model.

4. Functions and Responsibilities

This section provides overview of some of key roles, functions and responsibilities that are considered as part of the implementation of the SACSF.

4.1 Cabinet

Cabinet is responsible for:

- Approval of the SACSF and any updates to the Principles or Policy Statements.
- Noting annual SACSF attestation report.

4.2 Senior Management Council

Senior Management Council is responsible for:

- Noting the SACSF and approving its submission to Cabinet.
- Noting annual SACSF attestation report and approving its submission to Cabinet.

4.3 ICT and Data Board

The whole of government ICT and Data Board is responsible for:

- Endorsing the SACSF and overseeing the annual review of the SACSF and any subordinate documentation.
- Noting annual SACSF attestation report and approving its submission to the Senior Management Council.
- Noting agency Tier selection.

4.4 South Australian Government Cyber Security Steering Committee

The South Australian Government Cyber Security Steering Committee is responsible for:

- Endorsing the SACSF and overseeing the annual review of the SACSF and any subordinate documentation.
- Noting annual SACSF attestation report and approving its submission to the ICT and Data Board.

4.5 The Department of the Premier and Cabinet

The Department of the Premier and Cabinet's Office for Cyber Security are responsible for:

- Maintaining and communicating the SACSF across agencies.
- Providing expertise and guidance to agencies with regard to implementing the SACSF.
- Ensuring a consistent approach to the implementation of the SACSF.
- Administering the SACSF attestation process.

4.6 Agency Chief Executives

The agency Chief Executive (or equivalent) is ultimately accountable for the successful operation of the agency's Cyber Security Program (CSP). The Chief Executive is accountable for:

- Definition of the agency's cyber security risk appetite.
- Selection of the agency's SACSF tier level.
- Assigning ownership of the agency's CSP.
- Reviewing and approving the SACSF attestation.
- Assigning suitable and sufficient cyber security resources.

4.7 Agency Senior Leadership

Senior leadership comprising the agency's executive leadership team or equivalent is responsible for providing support and resources for the CSP and championing organisational commitment to improving the cyber security culture of the agency.

4.8 Cyber Security Program Owner

The CSP owner is responsible for the successful operation of the CSP and is expected to:

- Provide CSP visibility as required to senior leadership.
- Monitor and report to senior leadership on the effectiveness of the CSP.
- Facilitate the provision of adequate training to ensure sound cyber security practices are understood by all personnel and effective cyber security controls are implemented.
- Review and approve Agency Security Committee recommendations on major security incidents, risks and risk treatment plans, adequacy of response and controls, security audits, and corrective actions and improvements taken.
- Review and approve core cyber security documentation and artefacts.

Note: *It is expected that the Cyber Security Program Owner function will be fulfilled by the Agency Security Executive (ASE), however this decision is to be based on the individual requirements of the agency.*

4.9 Cyber Security Program Coordinator

The CSP Coordinator is responsible for the operations of the CSP and coordination of cyber security activities including:

- Responding to the direction of the CSP owner.
- Organising and chairing the Agency Security Committee.
- Ensuring the activities documented in the cyber security calendar are scheduled, updated and performed.

- Escalating any issues, as necessary, to the CSP owner.
- Monitoring cyber security incident investigations and corrective actions.
- Highlighting major cyber security incidents to the Agency Security Committee.
- Ensuring operational cyber security activities are performed.
- Coordinating with external security vendors and specialists for expert advice.
- Reporting on various aspects of the CSP including security metrics, outstanding issues, and progress of the actions in risk treatment plans.

Note: *It is expected that the Cyber Security Program Coordinator function will be fulfilled by the agency Information Technology Security Adviser (ITSA), however this decision is to be based on the individual requirements of the agency.*

4.10 Agency Security Committee

The role of the Agency Security Committee is to act as the coordinator and adviser for all cyber security aspects in relation to the scope of the CSP, including:

- Responding to the direction of the CSP Owner.
- Ensuring the development and maintenance of, and adherence to, the agency's policies, procedures, work instructions and other operational documents to ensure compliance with the CSP.
- Reviewing security weaknesses and facilitating improvements to remediate cyber security risks identified by the agency risk management processes.
- Monitoring changes to services or deliverables for interested parties and reassessing any associated risks.
- Reviewing outcomes from cyber security incidents and associated corrective actions and improvements.
- Evaluating the results of internal and external audits and facilitating the required remedial actions.
- Communicating and providing guidance on implementation of cyber security policies, procedures, and other operational documents.

Membership may change based on operational requirements, and support and advisory groups can be invited as needed to attend Agency Security Committee meetings.

Note: *It is expected that the composition of the Agency Security Committee will be based on the individual requirements of the agency (e.g. an agency may have an existing governance committee in place that could consider security as part of its regular meetings).*

5. The Framework

The SACSF consists of **21** policy statements underpinning the principles of: ***Governance, Information, Personnel*** and ***Physical***.

PRINCIPLE ONE: GOVERNANCE		
Manage security risks and support a positive security culture, ensuring clear lines of accountability, strategic planning, assurance and review, and proportionate reporting.		
Leadership	Organisational Structure and Staff Responsibilities	Risk Management
Policies, Procedures and Compliance	Supplier Management	Audit and Assurance
PRINCIPLE TWO: INFORMATION		
Maintain the confidentiality, integrity and availability of all agency information and systems.		
Information Asset Identification and Classification	Incident Management	Resilience and Service Continuity
Access to Information	Administrative Access	Vulnerability Management
System and Software Acquisition	Secure Software Development	Network Communications
Cloud Computing	Mobile Device Management	Teleworking
Robust ICT Systems and Operations		
PRINCIPLE THREE: PERSONNEL		
Ensure employees and contractors are suitable to access South Australian Government resources and meet an appropriate standard of integrity and honesty.		
Personnel Security Lifecycle		
PRINCIPLE FOUR: PHYSICAL		
Provide a safe and secure physical environment for people, information and assets.		
Physical Security		

6. Principles and Policy Statements

Agencies and suppliers must consider and address each of the following 21 policy statements as part of their implementation of, and ongoing alignment to, the SACSF.

Appendix A lists each policy statement along with subordinate expectations and guidance that agencies and suppliers may consider. As referenced above, an implementation toolkit is also available that provides additional information, templates and tools that agencies can refer to.

PRINCIPLE ONE: GOVERNANCE
Manage security risks and support a positive security culture, ensuring clear lines of accountability, strategic planning, assurance and review, and proportionate reporting.
1.1: Leadership Senior leadership is ultimately accountable for the implementation and effectiveness of the agency's cyber security program. Senior leadership must be actively engaged in cyber security initiatives and champion cultural change. Senior leadership must demonstrate a commitment and understanding of the agency's cyber security program by providing an attestation of their current assessment against all mandatory requirements in the SACSF.
1.2: Organisational Structure and Staff Responsibilities A structure for managing cyber security must be embedded into the agency's governance framework. Roles and responsibilities for cyber security must be formally assigned by senior leadership, demonstrating commitment to providing suitable resources to manage the agency's cyber security program. Personnel and contractors must be provided with information and training to support awareness of their collective responsibility to foster a positive security culture.
1.3: Risk Management The agency must take steps to identify, understand, assess and manage cyber security risks to its critical processes and information assets. Cyber security risk management processes must be embedded within the agency's risk management framework and align to the risk appetite of the agency. Senior leadership must be aware of current and emerging cyber security risks to the agency.
1.4: Policies, Procedures and Compliance Cyber security policies and procedures must be in place and approved by senior leadership, providing management direction and support for cyber security in accordance with business requirements and relevant laws, regulations and contractual requirements, and the SACSF. The agency's suite of cyber security policies, procedures, and working documents must be reviewed regularly and socialised throughout the agency.

1.5: Supplier Management

Cyber security requirements must be included in all agreements with suppliers.

Processes for assessing and managing the risks that suppliers introduce must be embedded within the procurement and contract management functions in alignment with the agency's risk management framework.

1.6: Audit and Assurance

A program of cyber security assurance activities must be in place to evaluate the effectiveness of the agency's cyber security program and ensure cyber security controls are implemented and operated in accordance with the agency's policies and procedures, relevant laws, regulations and contractual requirements, and the SACSF.

PRINCIPLE TWO: INFORMATION

Maintain the confidentiality, integrity and availability of all agency information and systems.

2.1: Information Asset Identification and Classification

Information assets supporting critical processes must be identified, recorded and classified.

Processes must be place for labelling, storing, handling and disposing of assets in alignment with their classification.

Agencies must comply with SACSF Ruling 2 – Storage and Processing of information in outsourced or offshore ICT arrangements.

2.2: Incident Management

Cyber security incident response plans must be in place and aligned with an overarching incident management process to enable a consistent approach to the management of cyber security incidents.

Agencies must report to the Office for Cyber Security in line with the requirements of PC042 – Cyber Security Incident Management

2.3: Resilience and Service Continuity

Cyber security requirements must be included as part of agency business resilience planning and incorporated into periodic business continuity and service recovery testing.

2.4: Access to Information

Access to agency systems, applications and information must be based on business need, authorised by the information owner or delegated custodian and be limited to the minimum required for personnel to undertake their duties.

Secure authentication mechanisms must be in place to control access to agency systems, applications and information.

2.5: Administrative Access

Administrative access to agency systems, applications and information must be restricted to personnel with a specific business need which is validated on a periodic basis.

2.6: Robust ICT Systems and Operations

Standard operating procedures and technical controls must be in place to provide a consistent and secure approach to system administration, maintenance and configuration activities.

2.7: Vulnerability Management

Security vulnerabilities in agency ICT equipment, systems and applications must be identified and managed.

2.8: Network Communications

Network communications must be secured, ensuring agency information traversing internal and external networks and must be appropriately protected based on its classification and can only be accessed by authorised parties.

2.9: System and Software Acquisition

Cyber security requirements must be considered throughout the acquisition lifecycle for acquiring new systems and software.

2.10: Secure Software Development

Procedures for secure software development must be embedded into the software development lifecycle.

2.11: Cloud Computing

Risk assessments must be performed by the agency prior to implementing any cloud computing service in order to assess the benefits of the service balanced with the additional jurisdictional, governance, privacy and security risks associated with the use of such services.

2.12: Mobile Device Management

Technical and procedural controls must be in place to address the risks associated with the use of mobile devices including mobile phones, smartphones, tablets, laptops, portable electronic devices, portable storage and other portable internet-connected devices.

2.13: Teleworking

Secure practices for teleworking must be established and understood by agency personnel, with technical controls implemented to enable secure remote access to agency information.

PRINCIPLE THREE: PERSONNEL

Ensure employees and contractors are suitable to access South Australian Government resources and meet an appropriate standard of integrity and honesty.

3.1: Personnel Security Lifecycle

Agencies must assess the suitability of new and existing personnel in alignment with the classification of information to be accessed during employment.

Separating personnel must be made aware of their ongoing cyber security obligations.

PRINCIPLE FOUR: PHYSICAL

Provide a safe and secure physical environment for people, information and assets.

4.1: Physical Security

Protective security must be integrated in the process of planning, selecting, designing and modifying agency facilities for the protection of people, information and physical assets.

APPENDIX A: POLICY STATEMENTS AND TIER SPECIFIC EXPECTATIONS

In order to assist with implementation of the SACSF, each of the 21 policy statements are listed below along with tier specific expectations and guidance. The tier specific expectations outlined in this appendix are written as a set of increasingly complex treatments or controls spread across the four tier levels. For a tier one agency they should address the tier one expectations, whilst a tier four agency would be expected to consider the expectations of all the four tiers.

The following table provides an example of how to read the subsequent pages:

Policy Statement	Agency Tier Level	Expectations
1.1: Policy Statement Title Example Policy Statement (a)	One (b)	Example Expectation 1 (c) Example Expectation 2 (c) Example Expectation 3 (c)
	Two (b)	Example Expectation 1 (d) Example Expectation 2 (d) Example Expectation 3 (d)
	Three (b)	Example Expectation 1 (d) Example Expectation 2 (d) Example Expectation 3 (d)
	Four (b)	Example Expectation 1 (d) Example Expectation 2 (d) Example Expectation 3 (d)

1. This is the policy statement this is the top-level requirement that all agencies, regardless of size must address.
2. This is the agency tiering level that an agency will select based on their complexity, the criticality of their services, their risk appetite and a number of other factors as outlined in the SACSF Tier Selection section above.
3. This is the guidance and expectations on how a tier one agency would go about addressing the requirements of the policy statement. Agencies should consider the expectations. The Tier One expectations should also be considered as a baseline expectation for all agencies.
4. These are the increasingly complex standards or controls that should be considered by the higher tiered agencies. Importantly an agency at Tier Two should consider the Tier One expectations in addition to Tier Two. Whereas a Tier Three would consider Three, Two and One expectations and so on.

Principle One: Governance

Principle: The agency manages security risks and supports a positive security culture, ensuring clear lines of accountability, strategic planning, assurance and review, and proportionate reporting.

Policy Statement	Tier	Expectations

1.1: Leadership
Senior leadership is ultimately accountable for the implementation and effectiveness of the agency's cyber security program. Senior leadership must be actively engaged in cyber security initiatives and champion cultural change.
Senior leadership must demonstrate a commitment and understanding of the agency's cyber security program by providing an attestation of their current assessment against all mandatory requirements in the SACSF.
	One	• Senior leadership provides an annual attestation of the agency's current state of alignment to the SACSF; together with a plan to meet or maintain alignment to the agency's required tier level. The attestation covers:
		  ◦ Tasks completed during the reporting period.
		  ◦ Tasks to be completed during the new reporting period.
		  ◦ Cyber security program funding model.
		  ◦ Responsibility for completing the associated task.
		• Senior leadership allocates roles, responsibilities and resources to support and enable the agency's cyber security program.
		• Cyber security is regularly included in the agenda of an appropriate senior leadership body, ensuring discussion is focused on the progress of the cyber security program; and cyber security risks to the agency, both existing and emerging.

	Two	**As above**
	Three	**As above**
	Four	**As above**

Policy Statement	Tier	Expectations
1.2: Organisational Structure and Staff Responsibilities A structure for managing cyber security must be embedded into the agency's governance framework. Roles and responsibilities for cyber security must be formally assigned by senior leadership, demonstrating commitment to providing suitable resources to manage the agency's cyber security program. Personnel and contractors must be provided with information and training to support awareness of their collective responsibility to foster a positive security culture.	One	**Management Structure** | The management structure for cyber security is embedded into the agency's governance framework. | Oversight of the agency's cyber security program is assigned to an Agency Security Committee with a direct report to senior leadership. **Cyber Security Responsibilities, Training and Awareness** | The agency has appointed a senior leader accountable for cyber security to provide strategic level guidance for the agency's cyber security program and ensure compliance with cyber security policy, standards, regulations and legislation. | Responsibility for day-to-day cyber security operations is assigned and documented in policy and relevant position descriptions. | Cyber security education and awareness training is provided to all personnel and contractors during induction and at least annually thereafter, ensuring they are aware of their responsibilities regarding the appropriate use of agency information assets.
	Two	**Management Structure** | A dedicated Agency Security Committee is in place to enable effective communication and oversight of the agency's cyber security program. | The Agency Security Committee is attended periodically by a member of the agency's senior leadership. **Cyber Security Responsibilities, Training and Awareness** | Additional security training is provided to agency personnel who are in positions of trust, have heightened security responsibilities, or have increased risk profiles. | Personnel and contractors responsible for cyber security management and day-to-day operations maintain industry recognised certifications relevant to their role that have ongoing continuing professional education requirements or have been obtained within the prior five years. | The agency evaluates the performance of all workers with reference to cyber security responsibilities and performance requirements.
	Three	**Cyber Security Responsibilities, Training and Awareness** | Skills gap assessments are performed for cyber security and IT personnel responsible for implementing or managing technical security controls. Targeted training is provided for these personnel specific to the technologies in use within the agency. Where contractors or third-parties are used in place of internal resources, periodic vetting of competency is performed.

	Four	**Management Structure** • The agency operates an independently certified information security management system which covers the critical services of the agency and has implemented a formal business continuity management system. • The agency has formally appointed and defined responsibilities for an executive or senior manager solely responsible for cyber security.

Policy Statement	Tier	Expectations
1.3: Risk Management The agency must take steps to identify, understand, assess and manage cyber security risks to its critical processes and information assets. Cyber security risk management processes must be embedded within the agency's risk management framework and align to the risk appetite of the agency. Senior leadership must be aware of current and emerging cyber security risks to the agency.	One	Senior leadership has documented the agency's risk appetite. A risk management framework is in place and includes cyber security risk management processes. Cyber security risks are documented in an agency risk register; and are periodically reviewed by the Agency Security Committee. Cyber security risks are assessed and documented for all projects undertaken by the agency.
	Two	Cyber security risks are documented in a cyber security risk management tool maintained by security personnel and periodically reviewed by the Agency Security Committee.
	Three	**As above**
	Four	**As above**

Policy Statement	Tier	Expectations
1.4: Policies, Procedures and Compliance Cyber security policies and procedures must be in place and approved by senior leadership, providing management direction and support for cyber security in accordance with business requirements and relevant laws, regulations and contractual requirements, and the SACSF. The agency's suite of cyber security policies, procedures, and working documents must be reviewed regularly and socialised throughout the agency.	One	A suite of cyber security policies aligned to the requirements of the SACSF is in place and has been socialised throughout the agency. Significant changes to policies are communicated as they occur. Legal, statutory, regulatory or contractual requirements and the agency's approach to meet these requirements, including how they are monitored and kept up-to-date, are documented. Operating procedures supporting the agency's suite of cyber security policies are in place. Policies, procedures and working documents are version controlled. A cyber security calendar is maintained to schedule and track the status of the cyber security program**.**
	Two	Policies are reviewed every two years at a minimum.
	Three	Policies are reviewed annually at a minimum.
	Four	**As above**

Policy Statement	Tier	Expectations
1.5: Supplier Management Cyber security requirements must be included in all agreements with suppliers. Processes for assessing and managing the risks that suppliers introduce must be embedded within the procurement and contract management functions in alignment with the agency's risk management framework.	One	A formal supplier register is maintained by the agency. Processes for assessing and documenting cyber security risks that suppliers may introduce are embedded within procurement and contract management functions. Cyber security obligations to address identified risks are documented within supplier agreements. Agencies obtain assurance from suppliers that they have implemented controls to meet their cyber security obligations upon contract award and periodically thereafter.
	Two	**As above**
	Three	**As above**
	Four	Agencies obtain independent assurance from suppliers that they have implemented controls to meet their cyber security obligations upon contract award and annually thereafter.

Policy Statement	Tier	Expectations
1.6: Audit and Assurance A program of cyber security assurance activities must be in place to evaluate the effectiveness of the agency's cyber security program and ensure cyber security controls are implemented and operated in accordance with the agency's policies and procedures, relevant laws, regulations and contractual requirements, and the SACSF.	One	| Self-assessment assurance reviews of the cyber security program are performed at least annually by the agency. | Independent reviews are performed periodically in line with agency requirements. | Policy exemptions are formally requested, documented and monitored by the Agency Security Committee.
	Two	| A formal internal audit program is in place to assess alignment to the requirements of the SACSF. | Technical reviews of security of critical systems are planned and carried out using a risk-based approach.
	Three	**As above**
	Four	| Formal independent reviews of the cyber security program are undertaken at least annually.

Principle Two: Information

Principle: Maintain the confidentiality, integrity and availability of all agency information and systems.

Policy Statement	Tier	Expectations
2.1: Information Asset Identification and Classification Information assets supporting critical processes must be identified, recorded and classified. Processes must be place for labelling, storing, handling and disposing of assets in alignment with their classification. Agencies must comply with SACSF Ruling 2 – Storage and Processing of information in outsourced or offshore ICT arrangements.	One	Information assets supporting critical processes are identified and recorded in an information asset register. Information assets are formally assigned an owner. Information assets are classified by the asset owner in alignment with the South Australian Information Classification System.
	Two	Processes are documented and followed for labelling, storing, handling and disposing of assets in alignment with their classification.
	Three	**As above**
	Four	**As above**

Policy Statement	Tier	Expectations
2.2: Incident Management Cyber security incident response plans must be in place and aligned with an overarching incident management process to enable a consistent approach to the management of cyber security incidents. Agencies must report to the Office for Cyber Security in line with the requirements of PC042 – Cyber Security Incident Management	One	• Cyber security incident response is included in the agency's incident management policy, documenting responsibility for cyber security incident management. • Incident management plans and processes are socialised throughout the agency periodically, and testing is included in assurance activities performed by the agency. • Post-incident review procedures are performed, and evidence relevant to cyber security incidents is recorded and retained. • Agencies have a formalised process for reporting cyber security events to the Office for Cyber Security Watch Desk and assisting in the assessment process as required.
	Two	• Response plans are developed for high impact or high likelihood cyber security risks as documented in the agency's cyber security risk register. • Cyber security specialists are identified and obtainable for cyber security incident response through internal capability or arrangements with third party specialists. • Post-incident review procedures are followed that include assessment of root cause, and evidence of learnings and corrective actions performed to reduce the risk of a recurrence.
	Three	**As above**
	Four	• Cyber security incident management is embedded in the agency's formal business continuity management system.

Policy Statement	Tier	Expectations
2.3: Resilience and Service Continuity Cyber security requirements must be included as part of agency business resilience planning and incorporated into periodic business continuity and service recovery testing.	One	• Business impact assessments have been performed. • Cyber security requirements are included in critical process continuity plans. • IT service recovery plans aligned to the outage limits identified in the business impact assessments are in place. • IT service recovery plans are tested periodically as part of the assurance activities performed by the agency.
	Two	• A detailed business continuity plan is implemented. • Business continuity and IT service recovery testing includes periodic testing against cyber security scenarios.
	Three	**As above**

	Four	• A formal business continuity management system is in place and includes:
		  ○ Emergency and crisis management
		  ○ Incident management
		  ○ Business continuity
		  ○ Business impact assessments
		  ○ Disaster recovery
		  ○ IT service recovery
		• Cyber security elements of the business continuity management system are tested annually at a minimum.

Policy Statement	Tier	Expectations
2.4: Access to Information Access to agency systems, applications and information must be based on business need, authorised by the information owner or delegated custodian and be limited to the minimum required for personnel to undertake their duties. Secure authentication mechanisms must be in place to control access to agency systems, applications and information.	One	**Access Provisioning** | Physical or logical access to agency information assets is provided based on business need. | The processes to provision access to systems and applications in use within the agency are documented. **Authentication and Traceability** | All users have unique accounts providing traceability of actions within critical systems and applications. | Secure virtual private networks and multi-factor authentication are used to remotely access the agency's IT environment. | Password standards (complexity, minimum length, maximum age) are documented and implemented on all systems and applications. **Access Reviews** | Reviews of general user access are performed at least annually for the network and all critical applications. **Termination of Access** | Terminated user's access is revoked within defined timeframes.
	Two	**Authentication and Traceability** | Multi-factor authentication is required to authenticate all users in positions of trust.
	Three	**Authentication and Traceability** | Multi-factor authentication is required to authenticate users to cloud based solutions such as Office 365. | Certificate based authentication is implemented to identify authorised workstations connected to the agency's network. **Termination of Access** | Access of terminated personnel is revoked immediately upon departure.
	Four	**As above**

Policy Statement	Tier	Expectations
2.5: Administrative Access Administrative access to agency systems, applications and information must be restricted to personnel with a specific business need which is validated on a periodic basis.	One	**Access Provisioning** | Users are assigned a dedicated privileged account to be used solely for tasks requiring privileged access. | Documented policies restrict the use of privileged accounts from reading emails, accessing the internet and obtaining files via online services. | Local administrative privileges on workstations are removed. **Access Reviews** | Reviews of privileged user access are performed at least every 6 months. **Authentication and Traceability** | Privileged account actions deemed high risk by the agency are logged and monitored for unusual activity. | Password standards (complexity, minimum length, maximum age) for privileged accounts are documented and implemented on all systems and applications. **Termination of Access** | Privileged access is revoked immediately once there is no longer a specific business need for it.
	Two	**Authentication and Traceability** | Multi-factor authentication is required to authenticate privileged users.
	Three	**Access Reviews** | Privileged user access reviews are performed at least every 3 months. | Technical controls are in place to restrict the use of privileged accounts from reading emails, accessing the internet and obtaining files via online services.
	Four	**Access Provisioning** | A process exists such that there is formal request and approval of access associated with tasks requiring privileged actions, and privileged access is revoked upon completion of the task.

Policy Statement	Tier	Expectations
2.6: Robust ICT Systems and Operations Standard operating procedures and technical controls must be in place to provide a consistent and secure approach to system administration, maintenance and configuration activities.	One	**Standard Operating Procedures** | Standard operating procedures have been developed for all primary cyber security functions performed by agency personnel. **Change management** | A change management process is developed and implemented that includes: o Identification and documentation of changes to be made, o Approval required for changes to be made, o Implementation and testing of approved changes, and o Any actions to be taken before and after approved changes are made. **Backups** | Backup, restoration and preservation strategies are developed and implemented as part of business continuity, disaster recovery and digital preservation planning. | Backups of important information, software and configuration settings are performed at least daily and stored for at least three months. | Backup and restoration processes are tested annually. | Backups are stored offline, or online in a non-rewritable and non-erasable manner. **System Configuration & Hardening** | Macro settings within Microsoft Office are as follows: o Only signed Microsoft Office macros can execute, o Microsoft Office macros in documents originating from the Internet are blocked, and o Microsoft Office macro security settings cannot be changed by users. | Web browsers are configured to block or disable support for Flash content, web advertisements and Java from the Internet. | Technical controls are in place to restrict non-privileged users from installing software.

	Two	**Backups** | Full back up and restoration processes are tested when fundamental IT infrastructure changes occur. **System Configuration & Hardening** | Application whitelisting is implemented on all workstations and servers to restrict the execution of executables and software libraries to an approved set. **Event Logging and Monitoring** | An event logging strategy is developed and implemented covering events to be logged, logging facilities to be used, event log retention periods and how event logs will be protected. | A centralised logging facility is implemented, and systems are configured to save event logs to the centralised logging facility as soon as possible after each event occurs. | An accurate time source is established and used consistently across systems and network devices to assist with the correlation of events. **System Redundancy** | Redundancy is built into systems commensurate with the system availability requirements identified as part of the business impact assessments.
	Three	**System Configuration & Hardening** | Application whitelisting is implemented on all workstations and servers to restrict the execution of executables, software libraries, scripts and installers to an approved set.
	Four	**System Configuration & Hardening** | Controls are in place to isolate critical systems. | Critical system isolation is tested periodically.

Policy Statement	Tier	Expectations
2.7: Vulnerability Management Security vulnerabilities in agency ICT equipment, systems and applications must be identified and managed.	One	• Security vulnerabilities in applications and operating systems are patched or mitigated within **one month** of release for all workstations and servers. • Security vulnerabilities in applications and operating systems that are assessed as 'extreme' are patched or mitigated within **48 hours** of release for all workstations and servers. • There is a documented process for managing the risks associated with non-vendor supported applications and operating systems where they are required for a specific purpose. • A mechanism is in place to ensure compliance to patching requirements. Expected patching compliance rates are documented. • Malware detection and prevention tools are in place on workstations and servers.

	Two	• A vulnerability management strategy is in place that includes:
		  ○ Conducting vulnerability assessments and penetration tests for systems throughout their lifecycle to identify security vulnerabilities
		  ○ Analysing identified security vulnerabilities to determine their potential impact and appropriate mitigations or treatments based on effectiveness, cost and existing security controls
		  ○ Using a risk-based approach to prioritise the implementation of identified mitigations or treatments
		  ○ Monitoring information on new or updated security vulnerabilities in operating systems, software and ICT equipment as well as other elements which may adversely impact the security of a system.
		• Security vulnerabilities in applications and operating systems are patched or mitigated within **two weeks** of release for all workstations and servers.

	Three	**As above**
	Four	• Patching compliance reports are generated and provided to the agency by all relevant third parties.

Policy Statement	Tier	Expectations
2.8: Network Communications Network communications must be secured, ensuring agency information traversing internal and external networks and must be appropriately protected based on its classification and can only be accessed by authorised parties.	One	The agency's network architecture is documented showing the internal network structure and incoming/outgoing egress points. Information flows associated with critical processes are documented listing: o The type of information, o The classification of the information, o Who the information is being exchanged with, and o The controls in place to protect the information.
	Two	Risk assessments are performed for all information flows associated with critical processes, and appropriate controls applied.
	Three	**As above**
	Four	Information flow risk assessments are reviewed annually. Network segregation is implemented throughout the agency's network.

Policy Statement	Tier	Expectations
2.9: System and Software Acquisition Cyber security requirements must be considered throughout the acquisition lifecycle for acquiring new systems and software.	One	Security risks associated with system and software acquisition or significant system enhancements are identified, documented and managed as per the agency's risk management framework before the system and/or software is implemented into production. Where system acquisition relates to a cloud service, the requirements of 2.11 Cloud Computing are applied.
	Two	**As above**
	Three	**As above**
	Four	**As above**

Policy Statement	Tier	Expectations
2.10: Secure Software Development Procedures for secure software development must be embedded into the software development lifecycle.	One	• Software development, testing and production environments are segregated. • Secure coding practices are documented and followed. • Outsourced software development is supervised. • Security functionality testing occurs throughout development and prior to implementation. • Vulnerability assessments and penetration tests are conducted by suitably skilled personnel before systems are deployed, after significant changes have occurred, and at least annually or as specified by the system owner.
	Two	• Platform-specific secure programming practices are used when developing software, including using the lowest privilege needed to achieve a task, checking return values of all system calls, and validating all inputs. • Code reviews are performed by suitably skilled personnel prior to implementation. • Software developers are provided additional training relating to secure software development. • Workstations and accounts used for software development are managed in line with privileged access management procedures.
	Three	**As above**
	Four	**As above**

Policy Statement	Tier	Expectations
2.11: Cloud Computing Risk assessments must be performed by the agency prior to implementing any cloud computing service in order to assess the benefits of the service balanced with the additional jurisdictional, governance, privacy and security risks associated with the use of such services.	One	A risk assessment is performed before implementing any cloud service. Security risks associated with a cloud service are identified, documented and managed as per the agency's risk management framework before the cloud service is implemented.
	Two	**As above**
	Three	Formal Independent assurance reports relating to the risks associated with the cloud service are obtained on an annual basis where the cloud service is supporting: o Critical services, o Services with high availability or integrity requirements, o Services storing sensitive information or higher, or o Services with a moderate or higher risk profile.
	Four	**As above**

Policy Statement	Tier	Expectations
2.12: Mobile Device Management Technical and procedural controls must be in place to address the risks associated with the use of mobile devices including mobile phones, smartphones, tablets, laptops, portable electronic devices, portable storage and other portable internet-connected devices.	One	• Procedural controls have been established, outlining the mechanisms for protecting agency information stored on or accessed from laptops, mobile phones and removable storage devices. • Processes exist for requesting and authorising the use of personal mobile phones to access agency information such as emails. • Passphrases and/or PIN codes are in place on laptops and mobile phones used for accessing agency information. • Secure virtual private networks and multi-factor authentication are used to remotely access the agency's IT environment. • Multi-factor authentication is required when configuring mobile phones to access agency email accounts on initial set up and each time the user's account password is changed. • Encryption of storage is enabled for all laptops, mobile phones, and removable storage devices.
	Two	• A mobile device management solution is in place to ensure that appropriate controls are applied to all mobile phones, including personal phones used for work. • Remote wipe functionality is enabled for all agency laptops and mobile phones, including personal phones used for work.
	Three	**As above**
	Four	**As above**

Policy Statement	Tier	Expectations
2.13: Teleworking Secure practices for teleworking must be established and understood by agency personnel, with technical controls implemented to enable secure remote access to agency information.	One	• Teleworking procedures are established and socialised with agency personnel working offsite. • Travel devices are provisioned to agency personnel for international travel in alignment with the risks associated with the destination country/countries. • Technical controls are implemented to enable secure remote access to agency information assets.
	Two	**As above**
	Three	**As above**
	Four	**As above**

Principle Three: Personnel

Principle: Ensure employees and contractors are suitable to access South Australian Government resources and meet an appropriate standard of integrity and honesty.

Policy Statement	Tier	Expectations
3.1: Personnel Security Lifecycle Agencies must assess the suitability of new and existing personnel in alignment with the classification of information to be accessed during employment. Separating personnel must be made aware of their ongoing cyber security obligations.	One	• Background verification checks on all candidates for employment are performed in accordance with relevant laws, regulations and ethics, and shall be proportional to the business requirements, the classification of the information to be accessed and assessed risks. • Agencies assess and manage the ongoing suitability of their personnel in relation to the information accessed as part of their role. • Separating personnel are made aware of their ongoing cyber security obligations, and have their access to agency resources withdrawn, per user access management processes.
	Two	**As above**
	Three	**As above**
	Four	**As above**

Principle Four: Physical

Principle: Provide a safe and secure physical environment for people, information and assets.

Policy Statement	Tier	Expectations
4.1: Physical Security Protective security must be integrated in the process of planning, selecting, designing and modifying agency facilities for the protection of people, information and physical assets.	One	Physical security measures are in place to protect agency physical assets including people, information and facilities based on the classification of the information that they are approved for processing, storing or communicating.
	Two	**As above**
	Three	**As above**
	Four	**As above**

APPENDIX B: GLOSSARY OF TERMS

Term	Description
Agency	South Australian Government public sector agencies (as defined in the Public Sector Act 2009), that is, administrative units, bodies corporate, statutory authorities, and instrumentalities of the Crown. Each agency retains ultimate responsibility for all aspects covered by the SA Cyber Security Framework as it relates to a particular agency and its information assets.
Agency governance framework	The management structure used by the agency. Cyber security management will be embedded within the overall governance framework. Governance may be further described as: the decision-making processes that define expectations, grant power, or verify performance. It consists either of a separate process or of a specific part of management or leadership processes.
Certification	The process by which an Accredited certifying body issues a certificate of conformance to a given Standard to an individual or organisation.
Classification	The process by which information assets are labelled according to their business importance and sensitivity. Classification markings are used to indicate the value of the information.
Critical process continuity plan	Documented work-around plans for maintaining critical processes during a period of disruption.
Critical processes	Agency processes that, if not performed, would eventuate in the highest level of risk to the agency. This could include meeting critical needs of the agency or satisfying mandatory regulations and requirements.
Critical Service	Services that, if compromised, would result in significant damage to the physical, social or economic wellbeing of the State. Critical Services are not typically ICT services, they are services that an agency delivers to the community on behalf of the State Government.
Cyber Security	Measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means. (synonymous with ICT Security)
Cyber security program funding model	It is expected that there will be capital expenditure (CAPEX) during implementation of cyber security tasks and ongoing operational expenditure (OPEX) for ongoing maintenance and support.
Encryption	A process, which may be irreversible, of transforming information, particularly data, into an unintelligible form.
Exemption	Approval for exclusion from the implementation or use of a mandated document outlined in the SACSF.

Extreme vulnerability	Defined as: • the security vulnerability facilitates remote code execution, • critical business systems are affected, • an exploit exists in the public domain and is being actively used, and/or • the system is internet-connected with no mitigating controls in place.
Framework	A basic conceptual structure used to solve or address complex issues.
Governance	The exercising of authority or decision-making processes.
Guideline	A statement of desired, good or best practice.
Guidance	See Guideline.
ICT	Information and Communication Technology.
Incident	Any event which is not part of the standard operation of a service and which causes or may cause an interruption to, or a reduction in, the quality of that service and/or loss or corruption of information resulting in a breach or privacy or security.
Information assets	Any information or asset supporting the use of the information that has value to the agency, such as collections of data, processes, ICT, people and physical documents.
Information custodian	The individual or group assigned responsibility for managing a set of information.
Information owner	The individual or group responsible and accountable for a set of information. The information owner may, at their discretion, assign responsibility for management of the information to another person or group, also known as an information custodian.
ITSA	Information Technology Security Adviser is a Position of Trust as defined in the PSMF. This role is appointed by an agency or organisation to manage the security of information and ICT systems. ISMF Guideline 4b provides information about this role, including guidance on the selection of suitable persons to fill the role.
IT service recovery plan	Documented plans for restoring IT services following a disruption.
Mobile device	Mobile phones, smartphones, tablets, laptops, portable electronic devices, portable storage and other portable internet-connected devices.
Multi-factor	A method of authentication using separate mutually dependent credentials, typically “something you have” and “something you know”.

Periodic (periodically)	An event or action that must occur at prescribed intervals.
Policy	A statement of principles and/or values that mandate or constrain the performance of activities used in achieving institutional goals.
Portable Device (electronic, storage and/or internet-connected portable device)	A small, lightweight, portable, easy to use device which is capable of storing and transferring large volumes of data.
Position of trust	Any position or role within the agency with heightened levels of access to sensitive information or otherwise have increased risk profiles.
Regular (regularly)	An event or action that should occur at consistent intervals and is typically determined by Standard Operating Procedures or a Security Schedule.
Risk appetite	The level of risk the agency is willing to accept. Agencies will need to define what level of management response is required for each risk level, for example *Extreme/High Risk – Senior leadership response.* *Moderate Risk – Agency Security Committee response.* *Low Risk – Security management response.*
Risk Profile	An outline of the risks to which an organisation, or business unit within an organisation, is exposed. Most Risk Profiles identify specific risks, associated mitigation strategies and an overall assessment or grading of each risk.
Ruling	An official interpretive statement of general applicability issued and published by a recognised authority.
Agency security committee	The management group responsible for security. It is expected that Tier one agencies will assign this responsibility to an existing group, whilst Tier two – four agencies will create a dedicated Agency Security Committee.
Senior leadership	Generic term that may encompass the Agency Board, Senior Executive Members, Chief Executive, Agency Security Executive or equivalent.
Standard	A formal document that establishes uniform criteria, methods, protocols, processes and practices to meet policy requirements.
Strategy	A long-term plan of action designed to achieve a particular goal.
Supplier	Suppliers are defined as any individual, contractor, business partner, or agent not directly employed by a South Australian Government agency. Supplier access is defined as any local or remote access made by a supplier to Government IT assets. In terms of arrangements with suppliers, the scope extends to the various service delivery interfaces with those suppliers, as defined in contracts and/or service level agreements. It includes auditing of security services implemented by suppliers that have a material impact on the

	security of information managed by the agency, but otherwise excludes the suppliers' internal processes.
User	Anything, including persons and computer systems that access ICT resources.

APPENDIX C: GUIDANCE ON TIER SELECTION

Agency Chief Executives are ultimately accountable for their tier selection, and this tier selection will be noted by the whole of government ICT and Data Board on an annual basis as part of attestation processes.

The following table describes potential characteristics of agencies within each tier. These characteristics are not definitive and should be used as a guide only. Tier selection is aimed at providing additional guidance to help agencies to apply controls commensurate with the complexity and criticality of their agency.

Characteristics of a Tier Four Agency may include:

- Managing or maintaining information with a classification of Protected or higher.
- Providing services for the State of which an outage of more than four hours would result in catastrophic consequences for the State.
- Employing more than 2,000 personnel.
- Having a very low appetite for cyber security risk.

Characteristics of a Tier Three Agency may include:

- Providing technology services to other agencies.
- Managing or maintaining a large volume of information classified as Official: Sensitive, (e.g. personally identifiable information or health records).
- Providing services for the State of which an outage of more than 48 hours would result in catastrophic consequences for the State.
- Employing more than 500 personnel.
- Having a low appetite for cyber security risk.

Characteristics of a Tier Two Agency may include:

- Providing services for the State of which an outage of more than one week would result in catastrophic consequences for the State.
- Employing less than 500 personnel.
- Having a moderate or lower appetite for cyber security risk.

Characteristics of a Tier One Agency may include:

- Employing less than 200 personnel.
- Having a moderate or higher appetite for cyber security risk.

For more information:
Office for Cyber Security
Department of the Premier and Cabinet

T 1300 244 168
E officeforcybersecurity@sa.gov.au
W security.sa.gov.au