RECORDS AND INFORMATION SECURITY SCHEDULE

Contents

NOTES:

- Terms used throughout this schedule have the same meaning as defined in the *Public Finance and Audit Act 1987*, *Treasurer's Instructions 18 – Procurement,* and the Procurement Glossary.
- All values identified in the framework are in Australian Dollars and are GST inclusive.

RECORDS AND INFORMATION SECURITY SCHEDULE

Purpose

This schedule details the minimum requirements for identifying and managing records and information obligations. It also addresses information security risks that arise when public authorities engage with third parties and suppliers during procurement and contracting activities.

This schedule is not limited to procurements relating to information, communication or technology.

Interaction with other government instructions

This schedule details requirements for procurement and contracting activities under the SA Government Procurement Framework. The following public authorities are responsible for other functions directly related to the security of records and information.

	FUNCTIONS	AUTHORITY
Department of the Premier and Cabinet	Management of the South Australian Protective Security Framework (SAPSF) and policies: governance (GOVSEC), information (INFOSEC), personnel (PERSEC) and physical security (PHYSEC).	PCC030 - Protective Security in the Government of South Australia
	Lawful management of personal information ensuring individual rights to access and correct their information while balancing privacy with public interest.	Premier and Cabinet Circular 012 – Information Privacy Principles Instruction
Department of Treasury and Finance	Management of South Australian Cyber Security Framework (SACSF) and Control Agency and Hazard Leader for cyber crisis.	PCC030, *Emergency Management Act 2004* and State Emergency Management Plan
State Records of South Australia	Provision of advice and assistance to agencies with respect to records management practices.	*State Records Act 1997* and Contracting and Information Assets Standard
Crown Solicitor's Office	Drafting of contractual terms, conditions and definitions.	Government of South Australia's legal service

Public authority security governance

Under the SAPFS:GOVSEC1 all public authorities must have protective security arrangements in place addressing the 4 government security domains of security governance, information security, personnel security and physical security. The arrangements must include the appointment of an Agency Security Executive and an agency security plan.

Outsourcing the provision of goods and services, including information management, ICT services and contracted service delivery does not transfer operational risk from the State. Accountability for the security of records and information, and for the associated service outcomes, remains with the public authority.

RECORDS AND INFORMATION SECURITY SCHEDULE

Public officers should refer to their public authority's security policies and Agency Security Executive for support managing the security of records and information.

Public authorities should note that the SAPSF and SACSF apply to government only and not to external entities such as suppliers.

Understanding the security of records and information

Public authorities will support the protection of information and assets during procurement and contract management activities by identifying and managing risks, such as cyber threats imposed by suppliers across the supply chain.

Cyber security in this context involves processes, techniques, and risk management practices to safeguard:

- sensitive government information
- supplier-provided data and deliverables
- computer systems and networks used in service delivery
- software applications integrated into government operations

Government information is stored and transmitted through internal systems and external services, including those operated by suppliers. This creates a shared responsibility for security between government, the supplier, and their subcontractors and suppliers.

Unauthorised access or interference can lead to serious consequences, including:

- disruption of service delivery and business continuity
- corruption or fraud within procurement processes
- exposure of classified, private, or sensitive data
- reputational damage to government and suppliers
- significant financial loss
- foreign interference and national security risks

Identifying records and information

Public authorities will identify and document electronic or hardcopy records and information when planning a procurement and when transferring an executed contract from procurement to contract management. Identification and documentation must include all records and information that will be created, captured or required by suppliers, potential suppliers or the public authority during procurement and/or contract delivery.

RECORDS AND INFORMATION SECURITY SCHEDULE

Classifying records and information

Public authorities will classify any identified records and information according to 2 systems.

- The South Australian Information Classification System (under the SAPSF) determines how the information must be protected according to the business impact of that information being compromised:
  - UNOFFICIAL, OFFICIAL, OFFICIAL: Sensitive, PROTECTED, SECRET or TOP SECRET.
- The terms and conditions of the Standard Goods and Services Agreement or the Standard Not-for-Profit Funded Services Agreement (as applicable to the procurement):
  - confidential information, personal information, sensitive data.

Managing records and information

Public authorities will ensure that procurement risk management planning and contract risk management planning includes consideration of information security and records management, commensurate with the purpose and complexity of the procurement.

Management of records and information during procurement and contract management, and of any associated risks, will include establishing and documenting arrangements for:

- ownership, custody and transfer arrangements noting that ownership of official records remains with the public authority
- format(s), storage, retrieval, migration, sharing and accessibility
- protection against physical or technological risks
- disposal, retention or transfer at the end of the contract including the return of official records to the public authority
- protection against privacy, security, confidentiality and intellectual property risks
- monitoring and auditing processes of the contracted supplier's information management practices
- supplier notification of any actual or suspected security incident affecting government information, official records or systems used to deliver the contracted goods or services.

Public authorities will have proper systems in place for identifying, gathering, and recording relevant information in accordance with their contract management framework and the requirements of the *State Records Act 1997*, *Freedom of Information Act 1991* and Premier and Cabinet Circular 012 – Information Privacy Principles Instruction.

RECORDS AND INFORMATION SECURITY SCHEDULE

Disposing of records and information

Public authorities will ensure that disposal of any records and information during procurement and contract management, and at the end of a contract, complies with the requirements for the disposal of official records as set out in the *State Records Act 1997* including State Records Disposal Standard.

Public authorities must ensure that all government information held by suppliers or sub-contractors is returned, destroyed, or managed securely and in accordance with agreed arrangements at contract end or termination.

Public authorities must ensure that all supplier and sub-contractor access to government ICT systems, networks, records and information granted under the contract is revoked at contract end or termination.

Definition of records and information

The SA Government Procurement Framework uses the term '**records and information**' to refer to information assets and official records collectively.

Information assets are defined by the South Australian Cyber Security Framework (part of the South Australian Protective Security Framework) as:

- any information or asset supporting the use of information that has value to the agency, such as collections of data, ICT, people and physical documents.

Official records are defined by the *State Records Act 1997* as any record made or received by an agency in the conduct of its business, but does not include:

- a record made or received by an agency for delivery or transmission to another person or body (other than an agency) and so delivered or transmitted; or
- a record made by an agency as a draft only and not for further use or reference; or
- a record received into or made for the collection of a library, museum or art gallery and not otherwise associated with the business of the agency; or
- a Commonwealth record as defined by the *Archives Act 1983* of the Commonwealth, as amended from time to time, or an Act of the Commonwealth enacted in substitution for that Act; or
- a record that has been transferred to the Commonwealth.

Records are defined by the *State Records Act 1997* as any record that is:

- written, graphic or pictorial matter; or
- a disk, tape, film or other object that contains information or from which information may be reproduced (with or without the aid of another object or device).