Government of South Australia

Cloud Services Policy

DTF/P3.1

Across Government Policy

Purpose

The intent and purpose of this policy is to encourage Public Sector agencies where suitable to evaluate cloud services in ICT sourcing, procurement, or market approach. Suitability should be based on value for money in terms of innovation or productivity outcomes, business needs, resilience, and risk, as well as compliance with any relevant legislation, instructions, policies, standards, and rulings.

Scope

This policy applies to all South Australian Government Public Sector agencies (as defined in ICT Policy Statement 1 – Compliant Authorities).

Policy detail/Policy statements

The *Information and Communications Technology (ICT), Cyber Security and Digital Government Strategy 2020-2025* sets the strategic direction for the services consumed by the SA Government agencies, and all agencies are expected to align their strategies, plans and activities with this strategic direction to ensure optimal outcomes are achieved that best serves the people of South Australia.

This Strategy provides flexibility to the agencies to continue adopting cloud services where suitable. This policy makes it clear that the Government's strategic intent is to shift from 'Cloud Right' to a focussed simple and smart services that are accessible and inclusive that improve collaboration in a secure and trusted manner.

Public Sector agencies may evaluate cloud services in ICT sourcing, procurement, or market approach.

Evaluation must be driven by agencies business needs, resilience, and risk as part of their evaluation and should not be driven whether the solution is in the cloud.

Following should be considered as a part of the evaluation:

- value for money outcome for government – that is, value for money in terms of innovation and productivity outcomes
- government's obligations under relevant legislation, instructions, policies, standards, and rulings.

Aboriginal Impact Statement

The needs and interests of Aboriginal people have been considered in the development of this policy. There is no specific impact on Aboriginal people.

Roles and responsibilities

Position title or unit/team	Listed responsibilities
Chief Executive	Responsible for the effective implementation of, and compliance, with this policy within their agency.
Deputy Chief Executives, Executive Directors, Directors and Managers	Responsible for ensuring • the policy is implemented and observed by staff • staff are fully informed of their obligations and responsibilities under the policy, and trained where required • contracts and agreements with service providers require adherence to DPC policies whilst conducting DPC business • any reporting requirements are met.
Team leaders and Supervisors	Responsible for ensuring that the policy is observed by staff and that business processes support the policy requirements.
All staff	Required to comply with the policy and any related procedures, and to play an active role in ensuring the compliance of others.

Reporting

Not relevant.

Definitions

Term	Definition
Cloud Services	A cloud service allows users of ICT to access a service through a network without the need to acquire, own, and operate dedicated infrastructure, software and facilities. Further detail can be found in the definition of cloud computing provided by the United States National Institute of Standards and Technology (NIST). This includes definitions of: • essential characteristics of cloud services • service models – e.g. Software as a Service, Platform as a Service, etc. • deployment models – e.g. private cloud, public cloud, hybrid cloud, etc.
Public Sector Agency	An internal to government entity, including administrative units, bodies corporate, statutory authorities, and instrumentalities of the Crown, as defined in the *Public Sector Act 2009 (SA)*.

Related Documents

- Whole of Government ICT, Cyber Security and Digital Government Strategy 2020-2025
- NIST Definition of Cloud Computing
- ICT Policy Statement 1: Compliant Authorities
- ICT Ruling 1: Governance – Exemptions
- SACSF G3.0 Guideline for Engaging suppliers and cloud security
- SACSF Ruling 2.1 Offshore Data Storage and Processing
- Personal Information Breach Guideline (available to SA Government personnel only)

Document Control

Approved by	OICO Programs, Projects and Procurement Steering Committee	Version	2.1
Approved date	August 2022	Next review date	August 2024
Original date of approval	April 2015	Compliance	Mandatory
Objective ID			
Contact:	Government Technology Services		
Contact email	acrossgovernmentictservicedesk@sa.gov.au		

Licence



With the exception of the Government of South Australia brand, logos and any images, this work is licensed under a Creative Commons Attribution (CC BY) 4.0 Licence. To attribute this material, cite the Office of the Chief Information Officer, Department of Treasury and Finance, Government of South Australia, 2026.