Premier and Cabinet Circular

PC 004 – ICT, DIGITAL AND CYBER SECURITY REQUIREMENTS

Effective from November 2023

Contents

Purpose statement 3
Context 3
Authority and accountability 3
Application 5
Direction and Guidance 5
Establishing Services 6
Protecting information assets 7
Governance 7
Exemptions 8
Monitoring and compliance 8
Distribution and publication 9
Document Control 9
For more information 9

Purpose statement

This circular outlines the framework within which South Australia (SA) Government agencies are to operate in order to optimise technology innovation and investment for whole of government when planning, developing and implementing ICT, digital and cyber security solutions and arrangements.

This circular applies to:

- all SA Government agencies and associated entities (including third party providers managing services for the SA Government's core ICT, digital and cyber security arrangements on their behalf), and
- all aspects of SA Government agencies' ICT, digital and cyber security solutions and arrangements that connect to trusted or un-trusted services external to agencies' logical network boundary. This includes, but is not limited to, equipment, software, network infrastructure, communications, security, applications, data management and managed service providers.

Context

SA Government's core ICT, digital and cyber security arrangements are delivered and supported through a central and comprehensive government-wide network.

These are high value/highly complex arrangements established through whole of government ICT contracts[1], mandated by Cabinet.

Having a mandated approach that before embarking on planning, developing and implementing ICT, digital and cyber security solutions and arrangements, agencies will:

- optimise the benefits of whole of government services and arrangements, and
- ensure solutions do not inadvertently jeopardise or compromise services and arrangements.

Any arrangements that agencies are considering to develop and implement that contradict the intent or requirements outlined in this circular must first seek an exemption (detailed below).

Authority and accountability

Role of Office of the Chief Information Officer and SA Government's ICT, Digital and Cyber Security setting

The Office of the Chief Information Officer (OCIO) in the Department of the Premier and Cabinet (DPC) is responsible for whole of government technology and cyber security

[1] Whole of government ICT contracts are managed by Strategic Procurement, Department of Treasury and Finance. These contracts are established to support the South Australian Government's ICT, Cyber and Digital Strategy developed by Office of the Chief Information Officer, Department of the Premier and Cabinet.

services that are relied upon by SA Government agencies. These services include internet and network connectivity, unified communications, collaboration platforms (such as the central Microsoft 365 platform), cyber security assurance, cyber security intelligence and incident response services.

OCIO serves agencies by:

- providing strategic leadership and operational expertise and resilience for core whole of government technology, collaboration, communication and cyber security services to ensure SA Government agencies can deliver important services for the community.
- leading the development of technology and cyber security strategies to ensure resilient, efficient, collaborative, and secure whole of government services in partnership with agencies.
- leading digital strategy and policy for SA Government, partnering with DPC's Major Programs' Digital Programs team to build and deliver services.

The services provided through OCIO deliver significant value to government and are detailed in OCIO's Strategy and Role Statement.

Agency Responsibilities

Agencies are responsible for their line of business applications, information assets and operational systems that support their agency specific business functions which may include services provided to other SA Government entities.

Agencies must ensure that:

- this circular is implemented and observed by employees and contractors so they can fulfil their obligations and responsibilities before planning, developing and implementing ICT, digital and cyber security solutions and arrangements, and
- any contracts and agreements with managed service providers adhere to this circular.

Where ICT, digital and cyber security solutions or requirements are, or have potential to be common to more than one agency, agencies must actively engage with OCIO to seek a solution that balances the need of the agency and the value to government as a whole. Preference must be given to appropriate sharing and re-use, rather than duplicating systems and infrastructure. Agencies must actively identify synergies and opportunities, manage duplication, avoid divergence from standards, and increase overall efficiency and effectiveness to maximise benefits to South Australians and other agencies.

Agencies must consider all aspects of this circular before they start planning, developing and implementing ICT, digital and cyber security solutions and arrangements that connect to trusted or un-trusted services external to the agencies' logical network boundary.

Application

Definitions

Across government	involving or impacting multiple or all government agencies.
Architecture	the complex or carefully designed structure of something.
Collaboration	the action of working with someone to produce something.
Digital/Digital Services	service(s) designed with customers and available online, mobile-ready, easy to use and accessible.
Framework	an architecture framework provides principles, practices and guardrails for deploying/implementing a technology or system.
Governance	system of decision-making, directing and controlling, through rules, relationships, policies, standards, systems and processes.
ICT (Information and Communications Technology)	resources used to acquire, process, store, communicate and disseminate information.
Pattern	an architectural pattern is a general, reusable solution to a common occurring solution/problem with design and implantation guidelines.
Policy	a position or judgment with an across government focus, that describes actions or behaviours that people are expected to follow.
Solutions and arrangements	Includes, but not limited to equipment, software, network infrastructure, communications, security, applications, data management, programs. Projects, initiatives, contracts and managed service providers
Strategy	a plan of action, or direction (with an across government focus), designed to achieve a particular goal.
Trusted and untrusted services	Are those services external to the agencies' logical network boundary including, but not limited, to equipment, software, network infrastructure, communications, security, applications, data management and managed service providers
Whole of government	involving or impacting most or all government agencies.

Direction and Guidance

Government's ICT, digital and cyber security environment is underpinned by robust strategies, frameworks and policies.

These documents establish the requirements for agencies when considering the planning, development and implementation of ICT, digital and cyber security solutions and arrangements.

The South Australian Government's ICT, Cyber and Digital Strategy was established with, and for agencies, and provides cohesive direction and objectives to guide

decisions in support of the government's long-term strategic vision for core whole of government services.

Agencies must align their ICT, digital and cyber security activities with this strategy.

Further, across-government ICT, digital and cyber security frameworks, policies, standards and guidelines are based on best practice, with many of them mandatory to not only assist agencies with their business needs and consistency across government, but also to ensure the ongoing protection, confidentiality, integrity and availability of government systems and networks.

Establishing Services

The OCIO Service Catalogue for whole of government services offers a range of ICT, digital (including citizen engagement) and cyber security mandatory and/or preferred business solutions that are available for agencies' use. These services:

- have been appropriately assessed for use in the government's ICT environment,
- are maintained as the most current service offering,
- comply with maintenance schedules and processes, and
- offer interoperability, security, resilience and reliable services to support agencies' business and services to South Australians.

Agencies must refer to the Service Catalogue before considering standalone solutions. If a solution is not included in the OCIO Service Catalogue, and will need to connect to trusted or un-trusted services external to the agencies' logical network boundary, agencies must consult with OCIO as:

- an alternate solution may be in development
- OCIO may be aware of an existing agency solution, a pre-defined framework or pattern that could be leveraged, or
- OCIO may advise on any anticipated and adverse effects on the government's ICT environment or connectivity.

Should agencies still need to plan, develop and implement an ICT, digital and cyber security solution or arrangement, agencies must:

- evaluate cloud solutions when considering or developing ICT solutions or arrangements. Cloud services present many opportunities, including increased accessibility and scalability, and the potential to reduce electronic storage and internal ICT capital investment.
- consult with OCIO (Architecture Review Group) to review solution designs to ensure compliance and compatibility with the government-wide enterprise architecture and network. Following consultation, it may be necessary to seek an exemption from an existing across-government ICT arrangement (ICT contract, policy, standard, notification or equivalent instruction). Refer, *Exemptions* below.

Protecting information assets

Government agencies must protect infrastructure, digital assets and citizen information against cyber threats, in accordance with *PC030 – Protective Security in the Government of South Australia.*

In particular, Chief Executives are accountable for the cyber security of their agency and must ensure that their agency conforms to:

- The South Australian Protective Security Framework (SAPSF); and
- The South Australian Cyber Security Framework (SACSF).

Agencies must provide an annual attestation outlining the extent to which they have implemented the SACSF and SAPSF.

Risk and Risk Assessments

Agencies must ensure that their ICT and digital solutions and arrangements are secure by design to safeguard infrastructure, information and assets and to ensure the government is able to reliably and securely deliver services to the community.

Agencies must complete a risk assessment for any new or amended ICT and digital solution and arrangement, which:

- has a requirement to connect to the SA Government network (refer StateNet Conditions of Connection and whole of government Enterprise Architecture); or
- seeks Exemption from a mandated across-government ICT arrangement (ICT contract, policy, standard, notification or equivalent instruction).

Agencies should also be aware that the environment in which agencies and third parties operate changes frequently and as a consequence, so do the risks associated with the networks and ICT systems they operate.

Agencies must review risk assessments for ICT and digital solutions and arrangements that connect to SA Government's network (StateNet) at least once every two years or when significant change occurs.

Agencies must take reasonable steps to identify, assess, understand and manage cyber security risks to its critical processes and information assets in accordance with the SACSF.

Governance

The government's ICT, digital and cyber security environment is reinforced by a robust whole of government executive governance structure that sets the leadership and standard for the planning, development and implementation of ICT, digital and cyber security solutions and arrangements.

The South Australian Government ICT, Digital and Cyber Security Governance Framework describes the governance structures and requirements for planning, development and implementation of ICT, digital and cyber security programs, projects and solutions in the SA Government.

The Governance Framework includes an Architecture Review Group. Should agencies have a requirement to plan, develop and implement an ICT, digital and cyber security solution or arrangement that has a requirement to connect to trusted or un-trusted services external to the agencies' logical network boundary, agencies must consult with the Architecture Review Group to review solution designs to ensure compliance and compatibility with the government-wide enterprise architecture and network.

Exemptions

Government's starting position is that no agency within the scope of a mandated across-government ICT arrangement (ICT contract, policy, standard, notification or equivalent instruction) should be permitted to implement an alternate solution. Agencies must consider re-engineering their work practices and changing their procedures, where required, to fit mandated across-government arrangements.

Agencies must sufficiently articulate and substantiate why they require an exemption, with specific reference to areas identified in the Exemption Application Ruling and Guideline. This includes undertaking an appropriate risk assessment and considering any impact on the SA Government's network (refer StateNet Conditions of Connection) and the whole of government Enterprise Architecture.

The Executive Director/Government Chief Information Officer, OCIO retains the authority to grant, deny or revoke any exemption application.

Monitoring and compliance

Failure to comply with this circular will be reported to the relevant agency Chief Executive or SA Government's Senior Leadership Committee (chaired by the Chief Executive, Department of the Premier and Cabinet) to determine appropriate action.

This includes any activities that unduly expose SA Government to:

- risk (i.e. cyber security, legislative, availability, contract breaches etc)
- reputational damage
- limit its ability for efficiency and effectiveness (i.e. cost, interoperability etc)
- unjustly increases government spend or disadvantages other agencies.

Dependant on the severity, non-compliance may also be escalated to the Premier (responsible for the ICT, digital and cyber security), Cabinet or other relevant bodies.

If agencies become aware of non-compliance to this circular, the non-compliance must be reported to OCIO.

Where it is reasonably thought that compliance has been breached, independent assessments may be undertaken on those agency activities. Independent assessments (including any risk assessments) will be on-charged to the agency. Agencies will be responsible and held accountable to rectify any compliance issues within reasonable and agreed timeframes. OCIO may direct or work with agencies (where possible) to rectify and ensure compliance, and report back through the above positions/bodies.

Distribution and publication

The Circular will be published on the DPC website and the OCIO will write to all Chief Executives and agency Chief Information Officers (or equivalent) when the Circular is published.

Document Control

Review number: 1
Review date: November 2023

Next review date: April 2026

For more information

Office of the Chief Information Officer
Department of the Premier and Cabinet

E OfficeoftheCIO@sa.gov.au
W dpc.sa.gov.au