ICT, Cyber Security and Digital Government Strategy - Update for 2023

Plan for 2020 to 2025

Government of South Australia

Department of the Premier and Cabinet

Introduction

The South Australian (SA) Government is committed to making our state a better place to live, work and do business, now and for generations to come.

The COVID-19 pandemic has demonstrated that the SA community, including businesses and individuals, as well as government agencies, rely upon secure, resilient and innovative ICT, cyber security and digital services.

The Department of the Premier and Cabinet (DPC) is responsible for providing a broad portfolio of ICT, cyber security and digital services to the community and the SA Government.

This bold and ambitious strategy outlines the aspirations and deliverables for SA over five years, and is designed to contribute to the success of broader SA Government strategies.

Due to the interdependencies between technology, cyber and digital services, this strategy brings together these three domains to ensure there is focus on the right priorities, in close collaboration with agencies.

The strategy is presented through the lens of four key principles that guide our actions: smart, simple, connected, and secure, and three priorities to enable the state to be: (1) accessible and inclusive, (2) collaborative, and (3) secure and trusted. These priorities are underpinned by internal enablers.

The strategy ensures services are designed, built and delivered around the needs of businesses and community as well as SA Government agencies.

It identifies the strategy's goals for the next two years to 2025.

Update for 2023

Foreword

The Office of the Chief Information Officer (OCIO), in DPC, leads the SA Government's technology, cyber security and digital government strategies and policies and is the central service provider for whole of government technology and cyber security services and platforms.

In 2023 we delivered several whole of government initiatives, including establishment and migration to the Microsoft 365 (M365) Operating Model to automate and improve security, productivity, and collaboration in the South Australian Government M365 central tenancy.

We consolidated and replaced a number of legacy arrangements, with the establishment of two new network panels, the Telecommunications Services Marketplace panel and Network Hardware and Services Marketplace panel, delivering enhanced flexibility in the way the government network is managed and supported. We have finalised and established the new Microsoft Enterprise Agreement for whole of government for the next three years.

We progressed exiting the Glenside Data Centre and decommissioning the site as a whole of government data centre facility in conjunction with government agencies.

We provided guidance and leadership to government agencies in the safe use of Large Language Model (LLM) artificial intelligence tools with the development of a new guideline which provides information on the limitations and risks of LLM models and includes a range of mitigating controls that agencies can adopt. An across government AI Governance Working Group has been established to consider the long-term implications of AI and provide recommendations on an appropriate AI governance approach for SA Government.

DPC is the appointed Cyber Crisis Hazard Lead for the state and we worked with industry sectors and government agencies to develop the Cyber Crisis Hazard Risk Reduction Plan as the overarching framework for cyber hazard mitigation.

We continue to establish communities of practice, with over 20 ICT interest groups across SA Government, actively participating and sharing expertise, knowledge, challenges and best practices between employees, contractors, vendors, and partners.

We are committed to continuing to deliver on our ambitious strategy and would like to acknowledge our agency colleagues and industry partners for their ongoing collaboration and partnership, which have allowed OCIO to establish and deliver critical technology and cyber security infrastructure that is contemporary, resilient, and innovative to enable SA Government agencies to serve the community.

Dr. Eva Balan-Vnuk
Chief Information Officer
Office of the Chief Information Officer



Our priorities:

1. Accessible and inclusive
2. Collaborative
3. Secure and trusted.

Vision

As a thought leader and provider of many across government technology, cyber security and digital government services, OCIO is working towards:

- Enabling South Australians to live and thrive in a digital world.
- Embedding a co-design approach in everything we do, to ensure SA Government's services are designed and built around the needs of businesses and the community.
- Providing leadership through strategy, partnership and action to ensure SA Government delivers smart, simple and secure services to businesses and the community.

Guiding principles

The following guiding principles are adopted when creating new services, modernising existing services, and supporting agencies and the community:

- **Smart** services that make the best use of modern technology and resources.
- **Simple** services that are easy to use.
- **Connected** services that deliver better shared outcomes.
- **Secure** services that ensure trust, privacy and peace of mind.

Our people

OCIO is led by:

- **Dr. Eva Balan-Vnuk** - Chief Information Officer
- **Will Luker** - Chief Information Security Officer
- **Ed Reynolds** - Director Cloud Services
- **Paul Tracey** - Director Infrastructure and Customer Service
- **Nici Smith** - Director Internal Operations and Governance.

OCIO has a highly skilled, diverse workforce to meet the demands of a constantly evolving technology, cyber security and digital landscape.

SA Government priorities

SA Government agencies are working collaboratively to accelerate the state's economic recovery from COVID-19, and to ensure the state is an attractive place to live and do business, through leveraging existing assets, and building new ones. OCIO actively collaborates and partners with agencies to achieve positive outcomes for the state, including and not limited to, the following initiatives:

1. Develop a more resilient and innovative cyber security industry centred in Adelaide's innovation hub, Lot Fourteen, through the Australian Cyber Collaboration Centre (A3C).
2. Address and reduce the cyber and digital skills gap by developing education, training and pathways through cyber security traineeships for government, development of cyber school curriculum, and other skills growth activities.
3. As a major end user of ICT platforms, cyber security and digital government services, ensure industry is aware and engaged with government's strategic direction.
4. Improve online accessibility of government services for people living with disadvantage or a disability, in partnership with other agencies.
5. Improve the state's cyber security posture by implementing the South Australian Cyber Security Framework (SACSF) across government, and improve the industry's awareness of the SACSF.

What the strategy strives to achieve:

As SA's lead agency and the service provider of many across-government technology, cyber security and digital government services, OCIO is working towards achieving the following:

1. Accessible and inclusive

Better access

Enable a better digital experience for government employees and the community.

Shared responsibility

Cultivate a collaborative cyber security approach that brings together all levels of government with academia and the private sector.

Seamless service delivery

Readying central digital services for the future.

Build resilience

Strengthen the prevention of, detection of, response to and recovery from cyber security threats and incidents.

2. Collaborative

A connected government

Enhance integration and collaboration across South Australian Government to deliver shared outcomes.

3. Secure and trusted

Contemporary architecture

Lift government's capability to make it easy for citizens and businesses to interact with government with a cloud-first approach.

Influence leadership

Strengthen the role of government in providing sound governance and clear accountabilities for a whole of government approach to cyber security.

Priorities:

1. Accessible and inclusive

Design and deliver technology, cyber security and digital services that are accessible and meet the needs of SA businesses, community and government.

The SA Government is aware that it can be difficult for individuals and businesses to transact with government. DPC is working to improve the way individuals and businesses interact with government through the Serving South Australia - One Stop Shop initiative. This will, over time, provide a seamless and personalised online service that brings together a user's interactions with the SA Government into a convenient single location.

This is a multi-year, multi-agency initiative that adopts a human centred design approach, consulting with users and government agencies as services are redesigned for a better experience.

In 2019, the SA Government was a finalist for the Australian Human Rights Awards for the development of a publicly available online accessibility policy and toolkit, to ensure government digital platforms can be accessed and used by citizens, regardless of disability, digital literacy, device or location. This initiative has also been awarded two Australian Access Awards, including Accessibility Initiative of the Year in 2019.

SA's approach to online accessibility has received further accolades including the Plain English Campaign's Internet Crystal Mark in 2019, 2020 and 2021, a nomination for the 2021 United Nations Public Service Awards, and a Zero Project Award in 2022.

SA Government websites provided by DPC are certified Web Content Accessibility Guidelines (WCAG) compliant, improving digital inclusion in South Australia.

Over the last decade, more than 125,000 South Australians have registered to provide feedback on government policies and initiatives through the YourSAy online community engagement platform.

YourSAy hosts over eighty consultations from different government agencies each year to gain insights, feedback and suggestions from South Australians on initiatives related to transport, education, environment, social services, economy and business, and technology.

Collaboration with other governments across Australia also brings benefits, such as the Memorandum of Understanding between the SA Government and the Commonwealth's Digital Transformation Agency, signed in December 2018, to allow SA to leverage the significant federal investment in the Trusted Digital Identity Framework, to make it easier for Australians to access services and transact with government.

SA Government's core network, StateNet, has provided significant value over the years, however now is the time to adopt zero trust network principles.

This modern approach, approved in the state's Connectivity Infrastructure Strategy in November 2021, will not only improve the state's security posture, it will also make it easier for agencies to adopt cloud-based services so agencies can be more responsive to the needs of their customers.

1. Accessible and inclusive

Design and deliver technology, cyber security and digital services that are accessible and meet the needs of SA businesses, community and government.

Aspirations by 2025

1.1

Deliver improved citizen and business interactions with government via the Serving South Australia - One Stop Shop initiative, including: a) A range of new online digital transactions with a consistent user experience b) Personalised dashboard to view credentials, transactions and transaction status c) Single digital identity for SA Government services including linkage with myGovID.

1.2

Support agencies to design new services incorporating digital inclusion, architecture principles and security from the start.

1.3

Deliver high speed, low cost, ubiquitous connectivity across more of South Australia.

1.4

Consistent user experience in transacting with government (between in-person, online etc), including the extension of operating hours in Service SA centres.

1.5

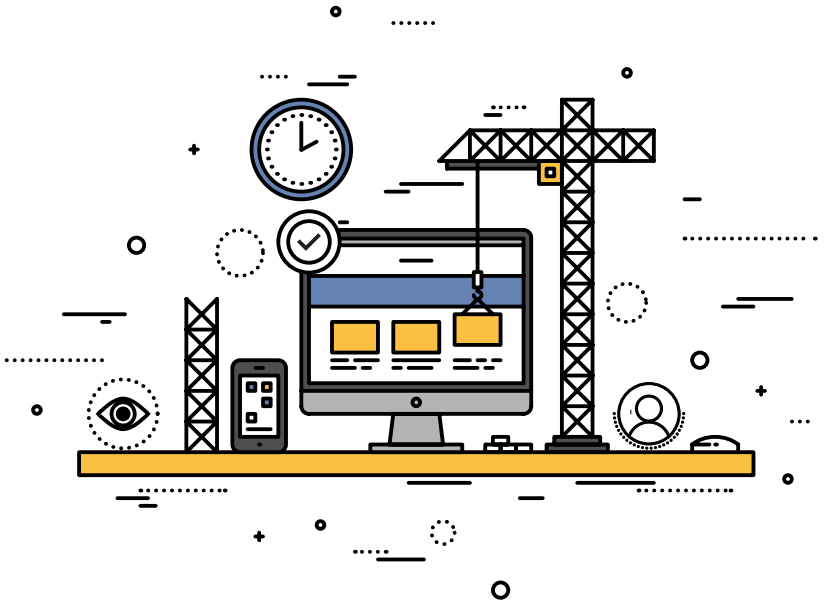
Deliver enterprise voice solutions based on agency user personas for consolidated investment, economy of scale and value realisation.

1.6

Active communities of practice across government, informing better ways of delivering services.

1.7

Provide a robust set of whole of government digital services, including surveys, community engagement, forms, websites and others as required.



Priorities:

2. Collaborative

Enable government innovation, efficiency and effectiveness through the provision of the latest digital collaboration tools, to produce better outcomes and services for citizens and businesses.

As a significant buyer of goods and services, the SA Government has an obligation to engage professionally and responsibly with partners and suppliers for the benefit of the state. A number of industry forums have been hosted over the last three years to share government's ICT, cyber security and digital government priorities, as well as host unique conversations with industry, such as the role of ethics in digital services, and the role of technology to support mind health and wellbeing.

Ongoing dialogue about this strategy with industry will ensure our partners and suppliers can better support us in achieving our strategic aspirations.

The SA Government recognises that industry has many innovations and approaches that can benefit the state and how we operate. Engaging at a strategic level with key partners and suppliers will increase the opportunity for government to adopt relevant new approaches and solutions that allow agencies to deliver better services to the South Australian community.

The SA Government acknowledges that private providers are best positioned to offer specific services, such as hosting and cloud-based services. Therefore it is intended that OCIO will cease offering hosting services to agencies by early 2024.

The SA Government has a set of unique assets that make inter-agency collaboration and communication seamless and secure, including the government's Microsoft 365 central tenancy used by the majority of agencies and managed by OCIO. As evidenced through COVID-19, rapid establishment of secure collaboration and communication environments that allow for inter-agency problem solving has been critical to delivering better services for South Australians.

The SA Government will build on the existing foundation of services to continue to improve the way agencies work together. OCIO will continue to provide technical and strategic leadership, functionality deployment roadmaps, and practical toolkits and resources that agencies can use to improve their own productivity and internal capabilities.

OCIO will leverage its unique perspective to bring together specialist communities of practice across government to inform decision making, identify new and emerging technological solutions, confirm core shared service end user needs for government, apply best practice across agencies, and to inform strategic priorities. OCIO will actively support the establishment and continuation of communities of practice, for example for enterprise architects, Microsoft 365 champions, community engagement specialists and those committed to enabling online accessibility.

Artificial Intelligence (AI) will have a significant impact on how society operates and how we serve our community as a government. OCIO will be the thought leader on Government's use of AI providing guidance and leadership to agencies via its whole of Government AI working group.

There is an ongoing need for government to provide modern, user friendly and efficient voice and unified communications services. It is intended that the set of voice and unified communications services provided by OCIO will consolidate based on agency user personas to ensure economy of scale, thereby enabling agencies to more efficiently and effectively deliver services to the South Australian community.

2. Collaborative

Enable government innovation, efficiency and effectiveness through the provision of the latest digital collaboration tools, to produce better outcomes and services for citizens and businesses.

Aspirations by 2025

2.1
Meaningful and streamlined engagement with the ICT industry through presentations at various forums to share SA Government's priorities and opportunities, aligned with an outcomes-based, early engagement approach.

2.2
Co-design initiatives with strategic ICT, digital and/or cyber security suppliers to deliver social and economic benefit to the state.

2.3
Lead the development of easily consumable services that make it easy for businesses to use a digital identity (partner with Commonwealth, agencies, business etc. to develop).

2.4
Continue to mature the model for service transformation to enable widespread agency adoption of and capability to transform service delivery for citizens and businesses.

2.5
Expand the identity ecosystem to encompass other sectors, including finance and retail.

2.6
Widespread agency adoption of contemporary network security approaches, including zero trust network principles for government systems and applications.

2.7
Continuously develop easily customisable toolkits to enable agencies to adopt new functionality as conveniently and quickly as possible (Microsoft 365).

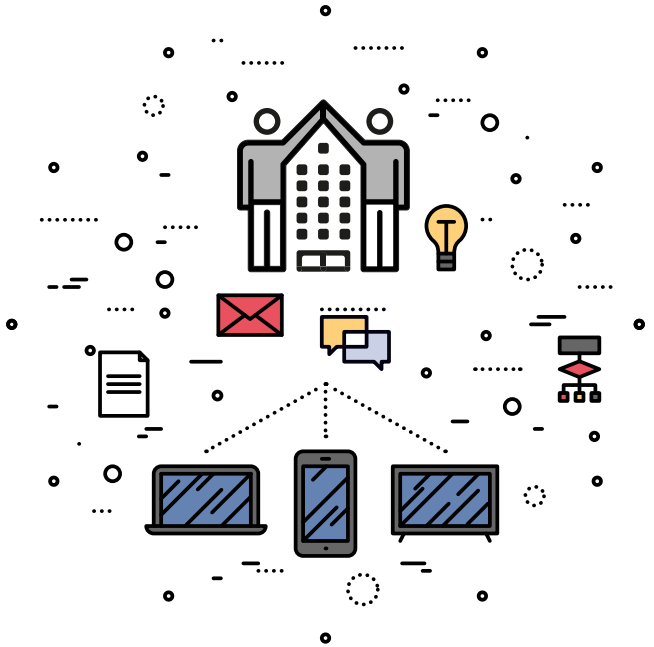
Aspirations by 2025

2.8
Deliver Enterprise Voice solutions based on agency user personas for consolidated investment, economy of scale and value realisation.

2.9
Exit government hosting services business.

2.10
OCIO provides leadership to SA Government in the adoption of new and emerging technologies.

2.11
Lead the development of a statewide connectivity investment strategy.



Priorities:

3. Secure and trusted

Protecting the safety and prosperity of South Australians online.

It is imperative that the SA Government demonstrates its commitment to ensuring the privacy and security of South Australians is respected and preserved, particularly as more transactions and interactions move to a more convenient and secure consent-based digital format.

This requires the SA Government to continue to improve its own security posture and capabilities, and support SA businesses to be more cyber resilient.

Citizens are increasingly looking to government and industry to deliver innovative and high-performing experiences which is driving rapid modernisation and reform across the public and private sectors.

With the increasing pervasiveness and complexity of digital, data and platform enabled services within government, there is a much greater level of sensitive data collection and aggregation, including both personal information and intellectual property. With that comes increased risk of data loss, fraud and identity theft.

To protect citizens, employees and the resilience of government services, it is essential that cyber security capability within the public sector continues to evolve and mature. This will require focus on uplifting core cyber capabilities in all parts of government, in addition to strengthening whole of government operational security services to improve our ability to effectively detect and respond to cyber threats which are growing in sophistication and complexity. This requires a holistic and well integrated approach which protects the collective attack surface within government.

The growing adoption of emerging technologies such as Cloud, Software as a Service (SaaS), AI and Automation, are creating new opportunities and increasing the use of shared responsibility service delivery models. Consequently, supply chain assurance, configuration management and the associated risks are also a key area of focus when securing SA's Digital Future.

Greater collaboration between industry and government will be important in reducing security risks associated with government third party service providers and securing critical infrastructure within SA.

Growing our future cyber talent continues to be a high priority for all of government to ensure that we are building the technical and leadership skills to secure government now and into the future.

Cyber risk does not observe geographic boundaries and accordingly, the SA Government will continue to work with colleagues and peers, nationally and inter-state to support positive national initiatives such as data enabled threat intelligence sharing and communities of practice.

3. Secure and trusted

Protecting the safety and prosperity of South Australians online.

Aspirations by 2025

3.1
Build community trust in transacting with government online.

3.2
Maintain support for key cyber security initiatives including the Australian Cyber Collaboration Centre (A3C), the Adelaide Joint Cyber Security Centre (JCSC) and the SA Node of AustCyber.

3.3
SA Government to continue to support the hiring of trainees and graduates in cyber security and related fields.

3.4
Drive collaboration, engagement and a common vision for cyber security across industry, academia, education and government in South Australia to ensure South Australia maximizes the opportunities that a cyber secure state could provide for, and ensure we are a 'partner of choice in an insecure world'.

3.5
Increase the maturity of the government's cyber threat intelligence capability to improve risk informed decision making around threats to government systems.

3.6
Improve the government's approach and ability to prevent and prepare for, as well as respond to and recover from, cyber security incidents including insider threats, through capability and capacity uplift across people, process and technology.

3.7
Lead the delivery of the SA Cyber Security Framework (SACSF) as the policy framework for the SA Government

Aspirations by 2025

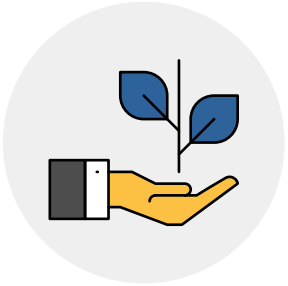
3.8
Bolster security operational capability for whole of government services managed by DPC.

3.9
Ensure government information, data and assets are appropriately managed, in line with their value, and agencies are equipped with the training and resources required to defend, detect and respond to security incidents.

3.10
Deliver a comprehensive, state-wide Cyber Hazard Risk Reduction program for SA that aligns with the state's emergency management arrangements.

3.11
Establish a strong risk-based approach to the security risk management of vendors and the government's supply chain.

3.12
Widespread agency adoption of contemporary network security approaches, including zero trust network principles for government systems and applications.



Enablers:

Internal to government approach

OCIO facilitates a whole of government governance framework for the SA Government that provides leadership, direction and advice to set the standards, policies and frameworks for the development of ICT, digital and cyber security solutions for SA Government, connecting agencies to share information and best practices.

An inaugural Satisfaction Survey was launched to agencies in late 2020 to gain valuable feedback on the services provided to agencies, and inform continuous improvements.

The insights also informed the technology, cyber security and digital government roadmaps that will influence the SA Government's investments in these areas. The survey was repeated in late 2021 and will be conducted biennially to ensure OCIO is responsive to feedback and delivers improved value to agencies.

OCIO will maintain a comprehensive Service Catalogue outlining services offered to agencies.

This will be updated regularly and include the addition of new services as they become available.

OCIO will continue to maintain frequent communications with stakeholders across government, focused on colleagues in ICT, digital and cyber security areas, and expanding to business stakeholders as relevant.

Enablers

We facilitate a whole of government governance structure that provides leadership, direction and advice to set the standards, policies and frameworks for the development of ICT, digital and cyber security solutions for SA Government, connecting agencies to share information and best practices.

Aspirations by 2025

4.1

Continue to engage with agencies through surveys, briefings, communities of practice, CIO forums etc. to inform improvements and priorities.

4.2

Digital government roadmap to inform government service improvements.

4.3

Deliver a government resourcing strategy (resourcing profile, employee value proposition, classification streams) to future proof government ICT, cyber and digital resourcing

4.4

Maintain the OCIO Service Catalogue, providing a comprehensive overview of services to agencies.

4.5

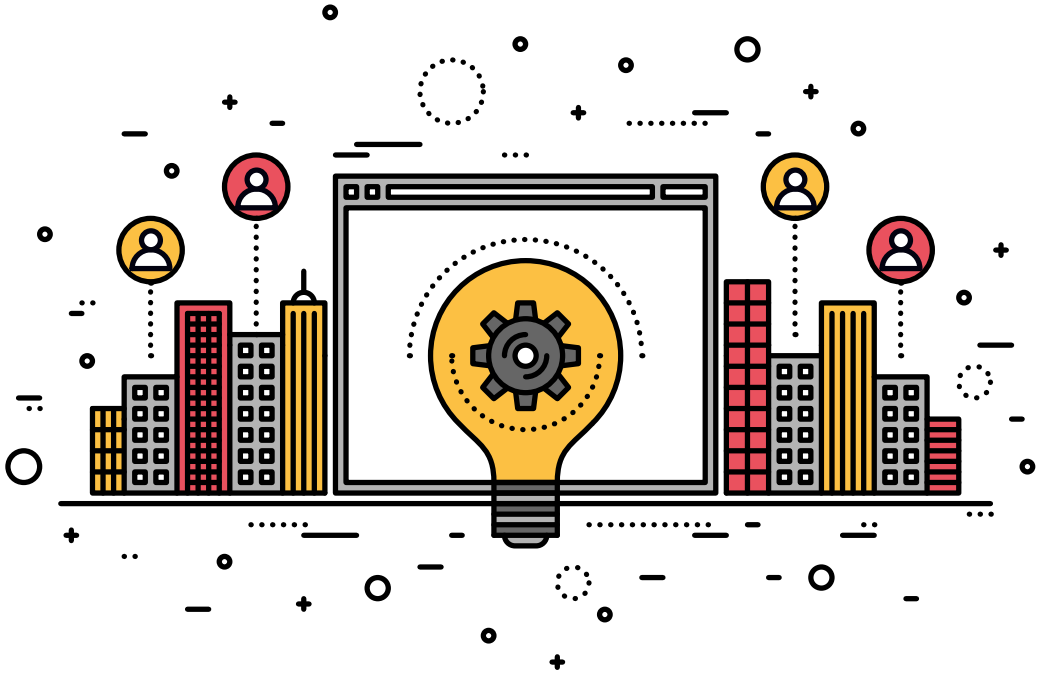
Optimise the maturity of product portfolio development and delivery.

4.6

Active communities of practice across government informing better ways of delivering services.

4.7

Provide a robust set of whole of government digital platforms, including surveys, community engagement forms, websites and others as required.



Government of South Australia

Department of the Premier and Cabinet

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