Cyber Safety Tasmania

Prevent. Protect. Play your part.

Tasmanian Government

Cyber Security Strategy 2024–2028

Digital Strategy and Services (DSS)
Department of Premier and Cabinet

Tasmanian Government

Enabling our digital future through trust and resilience, for the benefit of all Tasmanians

CONTENTS

In today's digitally connected world, the Tasmanian Government's commitment to cyber security remains unwavering.

Tasmanians are more connected than ever before.

Through digitally enabled environments we can now enjoy the convenience of services, information, education, and access to the global economy - all at our fingertips.

This digital transformation and innovation is essential for our economy to grow and our State to flourish.

The benefits of the evolving digital landscape are many, but as digitally enabled environments become increasingly interwoven in our everyday lives, so too are the cyber security risks to both organisations and individuals.

Cyber threats are becoming more complex, more difficult to detect and more costly to fix.

I am deeply passionate about, and committed to, safeguarding Tasmania's digital future.

Tasmanian Government Cyber Security Strategy represents this Government's dedication to protecting both your citizen information and importantly maintaining trust in government services.

Our vision is to enable our digital future through trust and resilience, for the benefit of all Tasmanians.

The Tasmanian Government Cyber Security Strategy embodies our dedication to protecting the wellbeing and prosperity of Tasmanians and maintaining trust in government services.

This strategy will enhance our cyber governance and strengthen cyber security through increased collaboration and resource allocation with our partners. Central to this is embedding a cyber security culture across all Government services, and strengthening cyber defences for our most critical services. We will leverage our partnerships across business and education to improve cyber resilience throughout the Tasmanian Government service delivery ecosystem.

At its core, this strategy will build a foundation of trust, privacy and resilience in digital services, for all Tasmanians.

I am proud to share the Tasmanian Government Cyber Security Strategy with you and the journey it embarks upon, where together we can create a safe, trusted and resilient digital future for all Tasmanians.

I encourage you to join me as we work towards a more cyber safe future for Tasmania.

Hon Madeleine Ogilvie MP

Minister for Innovation, Science, and the Digital Economy

OUR VISION

Enabling our digital future through trust and resilience, for the benefit of all Tasmanians

KEY PRINCIPLES

1 **The wellbeing and prosperity of all Tasmanians is our focus**

2 **We interact with community as one government**

3 **Security is an enabler for trust that underpins our digital services**

OUR GOALS

1 CYBER SECURITY LEADERSHIP

Enhance the Tasmanian Government cyber governance and operating model to strengthen the cyber security posture through more effective collaboration

2 EMBED SECURITY IN ALL GOVERNMENT SERVICES

Embed a strong cyber security culture throughout government, to strengthen cyber defences for government's most critical services and create opportunities for cyber talent within Tasmania

3 PARTNERSHIPS

Uplift our engagement with partners to strengthen cyber security across the Tasmanian Government service delivery ecosystem

TARGET ACTIONS

- Evolve our cyber governance and operating model to create a better response to changing cyber threat landscape
- Continuously improve cyber security tools and processes to accelerate digital transformation and innovation
- Increase whole of government visibility of risk to better prioritise resource allocation
- Enhance cyber security across whole of government to safeguard Tasmanians' services and information
- Enhance cyber security culture across the whole of government to ensure all staff participate in uplifting our cyber resilience
- Protect critical government systems and information by assessing and identifying new ways to address risks and threats
- Grow cyber talent through sustainable cyber pathways to ensure Tasmania develops a pool of local experts that can be leveraged by government and industry
- Develop Tasmanian Government Partnerships and Cyber Management Framework to strengthen the cyber defences across our entire value chain
- Define the Tasmanian Government Partnership arrangements to ensure all participants benefit and jointly uplift Tasmania's cyber awareness
- Strengthen industry partnerships to grow cyber talent and delivery

Within Australia, the ACSC* reports that governments comprise almost half of all security incidents reported to the ACSC*.

The ACSC* reports that the frequency of cyber-attacks has increased from 1 every 10 minutes in 2020 to 1 every 6 minutes in 2024.

*Australian Signals Directorate's Australian Cyber Security Centre.

Source: Australian Cyber Security Centre (ACSC) Annual Cyber Threat Report July 2020 – June 2024.

RESPONDING TO OPPORTUNITIES AND THREATS

In 2020 the Tasmanian Government launched a strategy aimed at leveraging the opportunities offered by emerging technologies, called 'Our Digital Future'. The strategy focuses on enabling digital services and engagement across the Tasmanian community, the economy and government.

As more and more services and information become available online, citizens must be able to successfully and safely navigate cyber space to participate freely in an inclusive digital environment.

Research continues to remind us that cyber threats are not only becoming more varied and frequent, but also harder to detect and more costly to remediate.

This is also increasingly driven by the growing complexity of cyber, greater integration of technology across government, and the wider ecosystem, including partners as well as citizens.

The ACSC reports that large data repositories like the ones operated by government are attractive to malicious actors, making these the most commonly attacked assets. In addition, perpetrators continue to threaten infrastructure assets as well as private citizens in different ways, with fraud, online shopping and online banking related breaches being the most common methods.

The development of strong cyber defence capabilities is a critical enabler for web-based government services.

The Tasmanian Government is acutely aware of its leadership role as a driver and enabler in the development of a broader, state-wide capability.

As a consequence, the Tasmanian Government will expand its existing cyber awareness programs to uplift the cyber and digital literacy of Tasmanians, Tasmanian businesses and our service delivery partners.

Partnerships with business and educational facilities will provide further stimulus that will lead to the development of skilled resources, as well as allow government to co-create sustainable services and solutions with industry.

OUR PRINCIPLES GUIDE US AS WE DELIVER OUR STRATEGY

1 The wellbeing and prosperity of all Tasmanians is our focus

Any initiative we deliver must make a positive impact on the lives of Tasmanians.

2 We interact with community as one government

Our initiatives will create a more seamless experience with citizens and businesses interacting with government.

3 Security is an enabler for trust that underpins our digital services

We build security into every initiative from the ground up. Security is front of mind, not an afterthought.

OUR ACTION PLAN

Tasmanians are set to gain significant benefits from a digitally enabled environment: better, more convenient access to services and information, easier access to a global economy including world-class education.

On the flipside, this also brings Tasmania well within reach of global crime syndicates and malicious state actors. It is therefore critical to develop suitable multilayered defences for the whole of Tasmanian society, with government at its core.

As one of the largest organisations in the state, the Tasmanian Government is keenly aware of its central role in establishing a cyber resilient and aware society.

The first pillar of our cyber security strategy recognises this responsibility and continues to develop the strong leadership required to address the challenges efficiently and effectively.

Initiatives will focus on further refining the cyber governance, risk assurance and operating model that underpin our digital government services.

The second pillar of our cyber security strategy acknowledges that trusted and resilient government services must be grounded in a strong cyber resilient culture.

Programs will deliver cyber knowledge and skills, observability and information sharing, as well as offer pathways for the development of cyber security talent.

Finally, contemporary services rely on modern ecosystems combining the skills and knowledge of diverse partners. However, complex ecosystems also create new challenges, and the threat surface increases with every new partner.

The Tasmanian Government is committed to leveraging its partnerships across business and education to improve cyber resilience across the entire ecosystem. Together the initiatives supporting these three strategic areas of focus will build a foundation of trust, privacy and resilience in digital services for all Tasmanians.

OUR GOALS

1 CYBER SECURITY LEADERSHIP

Enhance the Tasmanian Government cyber governance and operating model to strengthen the cyber security posture through more effective collaboration.

DESCRIPTION

The Tasmanian Government understands that the response to the emerging cyber threat landscape requires the rapid evolution of our leadership and governance model, capable of developing and directing required resources in a timely and efficient manner.

This will be achieved through a closer alignment of resources, tools and processes across all government agencies, including the evolution of the Tasmanian Government cyber operating model, and efficient sharing of threat information as well as best practice.

The continuous improvement of the Tasmanian Government cyber incident response capability will remain a cornerstone of our cyber resilience approach. While our cyber security response remains grounded in the agencies' ability to secure their respective ecosystems, the added level of capability and service will significantly improve our cyber security posture.

This combination of a de-centralised service with a shared operating model will provide growth opportunities for Tasmanian cyber specialists, which will continue to underpin our local cyber security response.

TARGET ACTIONS

- Evolve our cyber governance and operating model to create a better response to changing cyber threat.
- Continuously improve cyber security tools and processes to accelerate digital transformation and innovation.
- Increase whole of government visibility of risk to better prioritise resource allocation.
- Enhance cyber security across whole of government to safeguard Tasmanians' services and information.

OUR GOALS

2 EMBED SECURITY IN ALL GOVERNMENT SERVICES

Embed a strong cyber security culture throughout government, to strengthen cyber defences for government's most critical services and create opportunities for cyber talent within Tasmania.

DESCRIPTION

Decisions that affect an organisation's cyber security posture are made by everyone, on every level of the organisation, every day. A strong security culture is therefore critical to creating and sustaining a resilient cyber environment.

The Tasmanian Government has recognised this and created a cyber security awareness program that is continuously updated to reflect latest intelligence about the cyber threat landscape.

Further efforts will be made to embed cyber security in every aspect of the design, implementation and operations processes across the Tasmanian Government service ecosystem.

This will be grounded in a risk-based approach, which recognises that not all assets can be equally protected at all times, and in response every organisation must recognise the value of each asset and develop suitable defences.

TARGET ACTIONS

- Enhance cyber security culture across the whole of government to ensure all staff participate in uplifting our cyber resilience.
- Protect critical government systems and information by assessing and identifying new ways to address risks and threats.
- Grow cyber talent through sustainable cyber pathways to ensure Tasmania develops a pool of local experts that can be leveraged by government and industry.

OUR GOALS

3 PARTNERSHIPS

Uplift our engagement with partners to strengthen cyber security across the Tasmanian Government service delivery ecosystem.

DESCRIPTION

The delivery of modern, web-based services requires a broad set of competencies, which is why most organisations leverage capabilities developed by partner organisations.

This allows fast, scalable access to critical skills and services, but also expands the attack surface and introduces new risks across the supply chain that are more difficult to assess and manage.

The Tasmanian Government will continue to work across its partner ecosystem to continuously review and where required adjust its cyber security posture.

In addition, the Tasmanian Government will actively seek opportunities to cooperate with local cyber security professionals to continue to leverage their skills in the ongoing defence of the government's assets and encourage the development of the pool of Tasmanian cyber professionals.

TARGET ACTIONS

- Develop Tasmanian Government Partnerships and Cyber Management Framework to strengthen the cyber defences across our entire value chain.
- Define the Tasmanian Government Partnership arrangements to ensure all participants benefit and jointly uplift Tasmania's cyber awareness.
- Strengthen industry partnerships to grow cyber talent and delivery.

For further information, contact:
Digital Strategy and Services (DSS)

Department of
Premier and Cabinet
GPO Box 123
Hobart TAS 7001

ISBN 978-1-925906-47-9