Tasmanian Government

Cyber Security Policy

VERSION 1.1

NOVEMBER 2022

Department of Premier and Cabinet

Tasmanian Government

Contents

Background

Cyber Security is the body of technologies, processes and practices designed to protect networks, computers, programs and information from attack, damage or unauthorised access. Protection of information, systems and services is critical to effective delivery of Tasmanian Government services, and maintenance of public confidence in these services.

Purpose

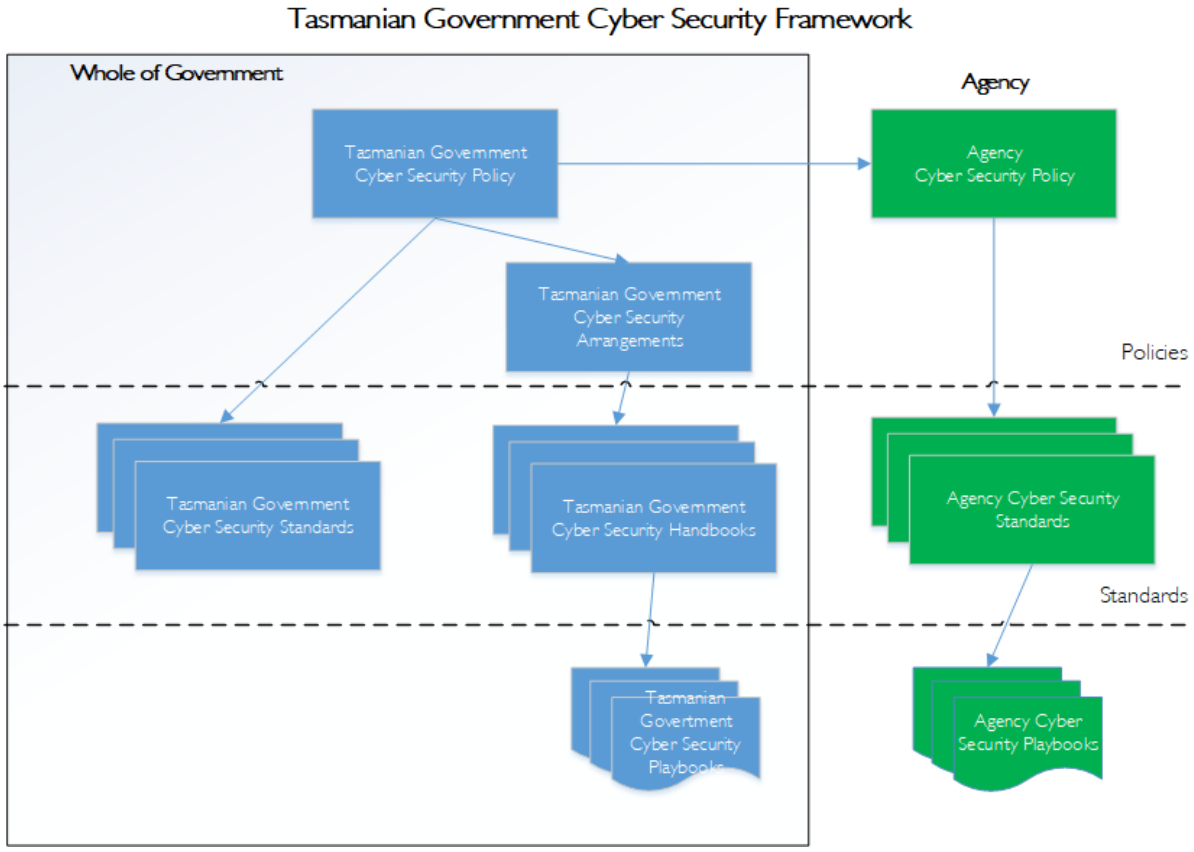
The purpose of this policy is to provide a consistent, risk-based approach to protecting Tasmanian Government information, systems and services from cyber security threats.

Context

This policy is the one of the principal documents of the Tasmanian Government Information Management Framework. The Framework is intended to be a coherent set of information management policies standards and implementation guidance for Tasmanian public sector bodies. This document sets out cyber security polices, principles and responsibilities as part of the Framework.

Tasmanian Government standards support this policy, including common approaches to identity and access to systems, and information security classification.

Associated documents with more detailed guidance support this policy, for example, cyber security incident response plans and cyber security incident response playbooks.



Benefits

Implementing this policy will:

- improve the Tasmanian Government's ability to identify and respond to cyber security risks
- improve cyber security risk management across Government
- raise cyber security awareness among staff
- increase confidence in Tasmanian Government digital services
- integrate cyber security risks into agency risk management frameworks
- enable increased information sharing with all levels of government and relevant external organisations.

Scope

This Policy currently applies to all Tasmanian Government agencies, as listed in Schedule 1 of the *State Service Act 2000*.

Other organisations may choose to adopt this Policy as good practice.

Policy statement

The Tasmanian Government will identify and manage cyber security risks to its information, systems and services throughout their lifecycle.

Policy principles

The Tasmanian Government Cyber Security Policy is founded upon the following underlying principles.

AWARENESS

Increased cyber security awareness enables staff at all levels to understand their responsibilities and identify and respond to cyber security risks.

COLLABORATION

Sharing cyber security knowledge across government improves cyber security capability and maturity.

ENABLEMENT

Cyber Security is a key enabler for digital transformation.

INTEGRATION

Integrating cyber security into business risk management frameworks, policies and procedures improves planning for, and responses to cyber security incidents.

PRIVACY AND SECURITY

Integrating cyber security into all digital systems and services improves privacy and security for consumers of Government services.

RISK

Adopting a risk-based approach allows the Tasmanian Government to adapt its cyber security risk management approach based on its risk tolerance.

STANDARDS

Aligning with national and international industry and Tasmanian Government standards provides a consistent, systematic and repeatable approach enabling collaboration across government and the private sector. Applicable international standards are AS ISO/IEC 27001 for cyber security management requirements; and AS/NZS ISO 31000 and AS/NZS ISO/IEC 27005 for risk management.

Responsibilities

Each Head of Agency or Chief Executive Officer is responsible for ensuring their agency identifies, measures and manages cyber security risks. This includes:

1. Developing, implementing and maintaining agency cyber security policies, standards and procedures that align with this policy.
2. Aligning agency cyber security risk management with this policy
3. Taking a risk-based approach to the management of cyber security practices, including the management of any risks associated with the cyber security practices of service providers engaged by the agency.
4. Contributing to the development and refinement of Tasmanian Government Cyber Security Standards.
5. Progressively implementing the requirements of the Tasmanian Government Cyber Security Standards, within the timeframes agreed by the Secretaries Board.
6. Managing and overseeing cyber security risks by the agency risk and audit committee or equivalent agency business risk governance committee.
7. Providing timely notification to the Tasmanian Government Chief Information Officer of cyber security events and incidents that could impact public confidence or affect the delivery of Tasmanian Government services.
8. Reporting annually to the Secretaries Board on the agency's implementation of the Tasmanian Government Cyber Security Standards and the agency's identification and mitigation of cyber security risks.

In situations where agencies are responsible for delivering whole-of-government or multi-agency services to other government organisations (for example, the services provided to other agencies by the Department of Premier and Cabinet through Service Tasmania) the Head of Agency or Chief Executive Officer of the service delivery agency is responsible for ensuring that the agency and/or the relevant service providers identify, measure and manage cyber security risk associated with the

delivery of these services. This includes ensuring that the service delivery agency and relevant service provider/s:

1. Deliver services in alignment with the Tasmanian Government Cyber Security Policy and associated cyber security documents
2. Develop, implement and maintain an Information Security Management System
3. Take a risk-based approach to the management of cyber security practices, including the management of any risks associated with the cyber security practices of service providers engaged by the agency
4. Progressively implement the requirements of the Tasmanian Government Cyber Security Standards, within the timeframes agreed by the Secretaries Board
5. Provide timely notification to the Tasmanian Government Chief Information Officer of cyber security events and incidents which could impact public confidence or affect the delivery of Tasmanian Government services
6. Report annually to the Secretaries Board on alignment of the whole-of-government / multi-agency services with the Tasmanian Government Cyber Security Policy, associated standards and identification and mitigation of Tasmanian Government cyber security risks.

The Tasmanian Government Chief Information Officer is responsible for:

1. Developing, implementing and maintaining whole-of-government cyber security policies, standards and procedures
2. Coordinating policy implementation across Government
3. Coordinating responses, the communication of information and the escalation of cyber security events and incidents, in alignment with the Cyber Security Incident Response Plan
4. Overseeing the cyber security requirements for whole-of-government digital projects and services.
5. Deliver whole of government services in alignment with the Tasmanian Government Cyber Security Policy and associated cyber security documents
6. Develop, implement and maintain an Information Security Management System for whole of government services
7. Take a risk-based approach to the management of cyber security practices, including the management of any risks associated with the cyber security practices of service providers engaged by Digital Strategy and Services
8. Define and manage the shared responsibility for cyber security risk to whole of government services.

Standards development

The development of Tasmanian Government Cyber Security Standards is an incremental and ongoing process.

Cyber Security standards are developed and refined through a consultative framework, led by a whole-of-government cyber security working group.

The working group reports to the Data and Digital Committee.

The Secretaries Board provides high-level oversight of the standards development process, including the establishment of timeframes for the agency-level adoption of each approved standard.

Definitions

Cyber Security	The body of technologies, processes and practices designed to protect networks, computers, programs and information from attack, damage or unauthorised access
Cyber Security Event	An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant
Cyber Security Incident	A single or series of unwanted or unexpected cyber security events that have a significant probability of compromising business operations and threatening information security
Information Security Management System (ISMS)	A set of policies, procedures and guidelines for systematically establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organisation's information security to achieve business objectives
Service Provider	An organisation, business or individual that provides services or products to an agency
Risk	Effect of uncertainty on objectives
Risk Management	Overall process of risk identification, risk analysis and risk evaluation
Risk Management Framework	Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation
Risk tolerance	An organisation's or stakeholder's readiness to bear the risk in order to achieve its objectives
Risk-based	Prioritised decision-making according to the risk level and the risk tolerance of the organisation

References

Australian Standard. AS ISO/IEC 27001 *Information technology – Security techniques – Information security management systems – Requirements*. Available on Standards Select through <www.dpac.tas.gov.au/divisions/digital_strategy_and_services/services/standards_select_online_service>.

Australian/New Zealand Standard. AS/NZS ISO 31000 *Risk management – Principles and guidelines*. Available on Standards Select through <www.dpac.tas.gov.au/divisions/digital_strategy_and_services/services/standards_select_online_service>.

International Standard. AS/NZS ISO/IEC 27005 *Information technology – Security techniques – Information security risk management*. Available on Standards Select through <www.dpac.tas.gov.au/divisions/digital_strategy_and_services/services/standards_select_online_service>.

Tasmanian Government Digital Transformation Strategy: *Our Digital Future* (2020). Available on https://www.digital.tas.gov.au

DOCUMENT HISTORY

Version	Date	Comments
1.1	Nov 2022	updated
1.0	Dec 2018	published

AUTHOR

Digital Strategy and Services division, Department of Premier and Cabinet

POLICY AUTHORISATION

Tasmanian Government Secretaries Board (previously Digital Services Board)

MONITORING PROGRESS OF POLICY IMPLEMENTATION

Monitoring will occur through the appropriate digital services governance arrangements.

POLICY MAINTENANCE

Digital Strategy and Services division, Department of Premier and Cabinet

POLICY ISSUED

December 2018

REVIEW DATE

No later than January 2025.

CREATIVE COMMONS STATEMENT