Tasmanian Government

Cybersecurity Policy

VERSION 1.0

DECEMBER 2018

Department of Premier and Cabinet

Tasmanian Government

Contents

Background

Cybersecurity 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

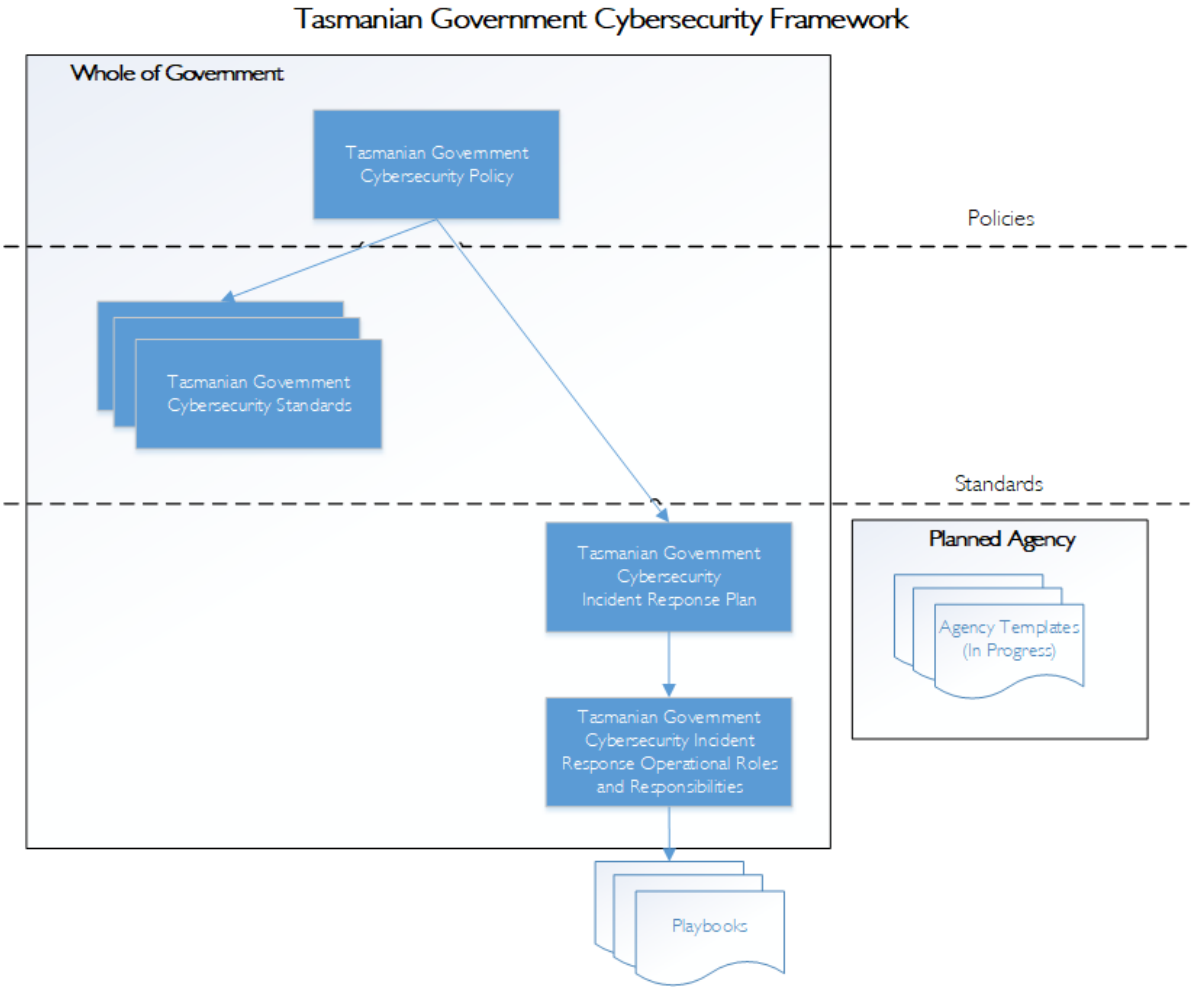
The purpose of this policy is to provide a consistent, risk-based approach to protecting Tasmanian Government information, systems and services from cybersecurity threats.

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 cybersecurity 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, cybersecurity incident response plans and cybersecurity incident response playbooks.



Benefits

Implementing this policy will:

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

Scope

This Policy 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 cybersecurity risks to its information, systems and services throughout their lifecycle.

Policy principles

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

AWARENESS

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

COLLABORATION

Sharing cybersecurity knowledge across government improves cybersecurity capability and maturity.

ENABLEMENT

Cybersecurity is a key enabler for digital transformation.

INTEGRATION

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

PRIVACY AND SECURITY

Integrating cybersecurity 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 cybersecurity 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 cybersecurity management requirements, 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 and manages cybersecurity risks. This includes:

1. Developing, implementing and maintaining agency cybersecurity policies, standards and procedures that align with this policy
2. Aligning agency cybersecurity risk management with this policy
3. Taking a risk-based approach to the management of cybersecurity practices, including the management of any risks associated with the cybersecurity practices of service providers engaged by the agency
4. Contributing to the development and refinement of Tasmanian Government Cybersecurity Standards
5. Progressively implementing the minimum requirements of the Tasmanian Government Cybersecurity Standards, within the timeframes agreed by the Digital Service Board
6. Managing and overseeing cybersecurity 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 cybersecurity events and incidents that could impact public confidence or affect the delivery of Tasmanian Government services
8. Reporting annually to the Digital Services Board on the agency's implementation of the Tasmanian Government Cybersecurity Standards and the agency's identification and mitigation of cybersecurity 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 and manage cybersecurity 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 Cybersecurity Policy and associated cybersecurity documents
2. Develop, implement and maintain an Information Security Management System
3. Take a risk-based approach to the management of cybersecurity practices, including the management of any risks associated with the cybersecurity practices of service providers engaged by the agency
4. Progressively implement the minimum requirements of the Tasmanian Government Cybersecurity Standards, within the timeframes agreed by the Digital Service Board
5. Provide timely notification to the Tasmanian Government Chief Information Officer of cybersecurity events and incidents which could impact public confidence or affect the delivery of Tasmanian Government services
6. Report annually to the Digital Services Board on alignment of the whole-of-government / multi-agency services with the Tasmanian Government Cybersecurity Policy, associated standards and identification and mitigation of Tasmanian Government cybersecurity risks.

The Tasmanian Government Chief Information Officer is responsible for:

1. Developing, implementing and maintaining whole-of-government cybersecurity policies, standards and procedures
2. Coordinating policy implementation across Government
3. Coordinating responses, the communication of information and the escalation of cybersecurity events and incidents, in alignment with the Cybersecurity Incident Response Plan
4. Overseeing the cybersecurity requirements for whole-of-government digital projects and services.

Standards development

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

Cybersecurity standards are developed and refined through a consultative framework, led by a whole-of-government cybersecurity working group.

The working group reports to the Digital Services Advisory Group, with all relevant standards submitted for approval by the Deputy Secretaries Digital Services Committee.

The Digital Services 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

Cybersecurity	The body of technologies, processes and practices designed to protect networks, computers, programs and information from attack, damage or unauthorised access
Cybersecurity 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
Cybersecurity Incident	A single or series of unwanted or unexpected cybersecurity 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.

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

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.

Tasmanian Government (2018) *Digital Service Board Terms of Reference V1.0*.

Tasmanian Government (2018) *Deputy Secretaries Digital Services Committee Terms of Reference V1.0*.

Tasmanian Government (2018) *Digital Services Advisory Group Terms of Reference V1.0*.

Tasmanian Government Information Management Framework policies, standards and toolkits (to be published).

Tasmanian Government Digital Transformation Strategy (to be published).

DOCUMENT HISTORY

Version	Date	Comments
I	12/12/2018	Approved by Digital Services Board
E	14/11/2018	Final draft updated for Digital Services Board approval
D	10/09/2018	Updated with feedback from Digital Services Advisory Group and other stakeholders
C	27/08/2018	Updated with feedback from stakeholders
B	10/08/2018	Consultation draft for feedback
A	13/02/2018	Initial draft

AUTHOR

Digital Strategy and Services, Department of Premier and Cabinet

POLICY REPLACES

The Tasmanian Government Information Security Policy. 2011.

POLICY AUTHORISATION

Digital Services Board

MONITORING PROGRESS OF POLICY IMPLEMENTATION

Monitoring will occur through the appropriate digital services governance arrangements.

POLICY MAINTENANCE

Digital Strategy and Services, Department of Premier and Cabinet

POLICY ISSUED

12 December 2018

REVIEW DATE

No later than January 2021, it may be updated before that date if required.

CREATIVE COMMONS STATEMENT