Tasmanian Government Incident Management Cybersecurity Standard

VERSION 1.0

SEPTEMBER 2020

Digital Strategy and Services
Department of Premier and Cabinet

Tasmanian Government

Contents

Purpose

This Tasmanian Government Incident Management Cybersecurity Standard (Standard) describes the minimum requirements for the development of a structured incident management framework. It will ensure that an agency can:

- respond effectively to suspected and actual cybersecurity events and incidents within the agency; and
- coordinate its response to whole-of-government cybersecurity events and incidents.

Scope

This Standard applies to all Tasmanian Government agencies, as listed in the *State Service Act 2000* Schedule 1.
Other Tasmanian Government organisations may choose to adopt this standard as good practice.

Implementation

Implementation of the controls within this Standard is mandatory unless an exception has been approved by the agency risk and audit committee (or equivalent).

Minimum Requirements

1. NOTIFICATION

Rationale: Timely notification of suspected or actual cybersecurity incidents allows agencies to respond quickly and minimise impact.

1.1. Agencies are to have defined procedures for reporting suspected or confirmed cybersecurity events and incidents

1.2. Agencies are to notify the Tasmanian Government CIO as per the Tasmanian Government Cybersecurity Incident Management Arrangements

2. PLANNING AND RESPONSE

Rationale: Incident response policies, plans and procedures support a systematic approach to dealing with cybersecurity events and incidents. This enables the effective response to events and incidents and the ability to learn from the response.

2.1. Agencies are to create incident management plans that detail the:

- a. roles, responsibilities, decision-making authority and summary of duties for stakeholders including incident response team
- b. register of important Contacts
- c. categorisation of incidents
- d. prioritisation of asset recovery
- e. escalation triggers and procedures
- f. communications and contact strategies
- g. procedures and playbooks to cover the stages of incident response. These must cover:
  - 2.1.g.1. business engagement procedures
  - 2.1.g.2. communications related procedures
  - 2.1.g.3. technical related procedures
- h. post-incident review process

2.2. Agencies are to maintain a register of critical business information assets/services which details:

- a. the Business Criticality of the asset and/or service
- b. Asset/Service Owner
- c. information locations

2.3. Contracts are to detail the agency's expectations regarding the service provider's and vendor's interaction with the agency incident management plan.

2.4. Agencies are to maintain a log of cybersecurity incidents in accordance with the agency disposal schedule.

3. READINESS

Rationale: To test the plans and procedures to ensure they are fit for purpose and effective; and that staff are prepared to respond to suspected or actual incidents

3.1. Agencies are to provide appropriate training to staff that may respond to cybersecurity events and incidents.

3.2. Agencies are to review incident response plans and procedures at least annually and after any major change.

3.3. Incident response plans and procedures are to be exercised at least annually to validate the plans and procedures and any changes required implemented.

Definitions

Business Criticality	The criticality of the data, asset or service to the business in terms of confidentiality, integrity and availability.
Asset/Service Owner	The person who is accountable for the security of the information in the asset and/or service. These are normally senior executives in the State Service (Directors, Deputy Secretaries or Secretaries etc.)
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
Cybersecurity incident management	A systematic and consistent approach to handling cybersecurity events and incidents.

REFERENCES

Australian Cyber Security Centre. *Australian Government Information Security Manual – Controls*. Available online at https://www.cyber.gov.au/acsc/view-all-content/ism.

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

ISO/IEC. ISO/IEC 27035-1 *Information Technology – Security techniques – Information security incident management – Part 1: Principles of incident management*. . Available on Standards Select through http://www.dpac.tas.gov.au/divisions/digital_strategy_and_services/services/standards_select_online_service.

ISO/IEC. ISO/IEC 27035-2 *Information Technology – Security techniques – Information security incident management – Part 1: Guidelines to plan and prepare for incident response*. . Available on Standards Select through http://www.dpac.tas.gov.au/divisions/digital_strategy_and_services/services/standards_select_online_service

Tasmanian Government. *Tasmanian Government Cybersecurity Policy*. http://www.dpac.tas.gov.au/__data/assets/pdf_file/0003/476706/Tasmanian_Government_Cybersecurity_Policy.pdf.

Tasmanian Government. *Tasmanian Government Cybersecurity Incident Management Arrangements*. Available from Digital Strategy and Services.

DOCUMENT HISTORY

Version	Date	Comments
1.0	15/09/2020	Approved by Deputy Secretaries Digital Services Committee

AUTHOR

Digital Strategy and Services, Department of Premier and Cabinet

STANDARD REPLACES

N/A

STANDARD AUTHORISATION

Deputy Secretaries Digital Services Committee

MONITORING PROGRESS OF STANDARD IMPLEMENTATION

Monitoring will occur through the appropriate digital services governance arrangements.

STANDARD MAINTENANCE

Digital Strategy and Services, Department of Premier and Cabinet

STANDARD ISSUED

15 September 2020

REVIEW DATE

No later than September 2023, it may be updated before that date if required.

COPYRIGHT STATEMENT