# Tasmanian Government Email and Messaging Cybersecurity Standard

VERSION 1.0

SEPTEMBER 2019

Department of Premier and Cabinet

Tasmanian Government

# Contents

# Purpose

This *Tasmanian Government Email and Messaging Cybersecurity Standard* (Standard) describes the minimum requirements for securing Tasmanian Government email and messaging systems.

Adoption of this Standard ensures that an agency can utilise its email and messaging systems to transmit, process and store information to an agreed whole-of-government level of security.

# Scope

This Standard applies to the configuration and management of inter-agency and externally-facing email and messaging systems by all Tasmanian Government agencies, as listed in Schedule 1 of the *State Service Act 2000*.

Other Tasmanian Government organisations may choose to adopt this standard as good practice.

# Implementation

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

# Minimum requirements

## 1. EMAIL AND MESSAGING INFRASTRUCTURE

*Rationale*: Securely configured email and messaging infrastructure can protect against the loss or unauthorised disclosure of data, the fraudulent use of legitimate addresses, and the potential interception or compromise of information.

1.1. Email and messaging systems are to be regularly risk-assessed and treated as part of each agency's risk management program.

1.2. Email and messaging systems will be hardened.

1.3. Email and messaging systems will have security patches applied at least monthly.

1.4. Open relaying of email will be disabled.

1.5. Audit logs for email and messaging systems, and mailbox use, are enabled.

1.6. DKIM records are to be configured for all email-enabled agency domains.

1.7. SPF and DMARC records are to be configured for all agency domains.

1.8. Agencies using third-party vendors to send emails or messages on their behalf are to include the third-party vendors in their SPF and DKIM records.

1.9. Anti-malware software is to be run on all email and messaging systems and is to be updated as recommended.

1.10. Agencies are to ensure all email and messaging network communications are encrypted where supported by both parties (sender and recipient).

1.11. Agency email hosting is to be within Australia.

1.12. Use of server-side rules to forward any email from a personal government mailbox to external mailboxes must be authorised.

## 2. CONTENT FILTERING

*Rationale*: The implementation of effective content filtering reduces the risk of disclosing information or allowing malicious code or spam into the environment when email and messages are transmitted between systems and networks.

2.1. All email inbound from outside the organisation is to pass through content filtering to identify and block malicious code and spam.

2.2. All message attachments are to be scanned for malicious code.

2.3. Emails received from an external source with an agency managed domain as part of the sender address must be blocked unless whitelisted.

2.4. Where an email is detected as suspicious by content filtering it is to be quarantined for the period of time defined by agency policy.

2.5. Where a message attachment is detected as suspicious it is to be deleted or have access blocked.

2.6. Agencies are to ensure content filtering of attachments by content types as per agency policy.

# Definitions

| | |
|---|---|
| Classified information | Information that needs increased security to protect its confidentiality |
| DMARC | Domain-based Message Authentication, Reporting and Conformance (DMARC) is an email authentication, policy and reporting protocol |
| DKIM | Domain Keys Identified Mail (DKIM) is an email authentication method designed to detect email spoofing |
| Hardened | Systems and services are configured as per good or recommended practice.<br>The process of hardening takes a risk-based approach to reducing the attack surface. For example, they run only applications required for the email and messaging system or necessary ancillary services and have all unnecessary services and data disabled or removed. |
| Mailbox(es) | A storage location for electronic mail, usually assigned to a single recipient |
| Malicious code | Any software that attempts to subvert the confidentiality, integrity or availability of a system; types of malicious code include logic bombs, trapdoors, trojans, viruses and worms |
| Messaging | A process of sending or receiving messages via electronic collaboration or instant messaging applications |
| Open relay | Simple Mail Transport Protocol (SMTP) server that allows third-party relay of email messages not sourced or destined for authorised domains |
| Phishing | Fraudulent emails or messages attempting to obtain sensitive information by masquerading as legitimate senders |
| Sensitive information | Either unclassified or classified information identified as requiring extra protection |
| SPAM | Unsolicited messages sent via email or messaging to large numbers of recipients for the purpose of advertising, phishing, business email compromise, nuisance or distribution of malicious code |
| SPF | Senders Policy Framework (SPF) is an email validation system designed to detect and block forged or spoofed emails |
| System | A related set of hardware and software used for the processing, storage or communication of information and the governance framework in which it operates |

## ATTRIBUTION

This work is a derivative or reproduces parts of the *Australian Government Information Security Manual.* Published by the Australian Cyber Security Centre https://www.cyber.gov.au/ism. Copyright Australia 2019.

## REFERENCES

Australian Cyber Security Centre (2019) *Australian Government Information Security Manual.* Available at: https://www.cyber.gov.au/ism.

Tasmanian Government (2018) *Tasmanian Government Cybersecurity Policy*. Available at: http://www.dpac.tas.gov.au/divisions/digital_strategy_and_services/dss_resources/Tasmanian_Government_Cybersecurity_Policy.pdf

## DOCUMENT HISTORY

| Version | Date | Comments |
|---|---|---|
| 1.0 | 17/09/2019 | 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

17 September 2019

## REVIEW DATE

No later than September 2022, but may be updated before that date if required

## COPYRIGHT STATEMENT

Copyright State of Tasmania 2019