Guiding checklist

Contents

[Introduction 3](#_Toc172539958)

[Security Governance 4](#_Toc172539959)

[Information Security 5](#_Toc172539960)

[People Security 6](#_Toc172539961)

[Physical Security 7](#_Toc172539962)

[Overall agency protective security 8](#_Toc172539963)

Author: Resilience and Recovery Tasmania  
Publisher: Department of Premier and Cabinet  
Date: June 2024

© Crown in Right of the State of Tasmania December 2022

# Introduction

This document has been prepared as a guide to support Tasmanian Government agencies with the implementation of Tasmania’s Protective Security Policy Framework (TAS-PSPF). The intention is to provide Agency Security Advisors (ASAs) with a quick snapshot of current security performance within the agency and aid in mapping some implementation activities.

The content of the checklist is based on the security outcomes of the TAS-PSPF and indicate best practice minimum protective security standards.

This document is not exhaustive and should not be the sole basis of assessing capability or risk for the agency. It does not replace in-depth security assessments required to fully understand your agency security posture.

Some topics to consider when using this document:

* Environmental scan of all premises’
* Location and site functions
* Monitoring the current threat environment
* Aggregate value of the agency’s resources
* Consequences of security breaches or incidents
* Business impact and ability to recover
* Proportionality and treatments according to risk environment

|  |  |
| --- | --- |
| Icon  Description automatically generated | Security Governance |

|  |  |  |  |
| --- | --- | --- | --- |
| **Security Governance** | | | |
| 1 | Does the agency have a Responsible Executive (RE) and ASA? | * Yes | * No |
| 2 | Does the Accountable Authority meet with the agency RE (or delegated security staff) regularly? | * Yes | * No |
| 3 | Does the ASA have adequate capability, capacity and resourcing to perform implementation activities in support of the TAS-PSPF? | * Yes | * No |
| 4 | Do agency security staff have sufficient knowledge of the TAS-PSPF and the Australian Government Protective Security Policy Framework? | * Yes | * No |
| 5 | Does the agency have an agency security plan that meets the requirements of GOVSEC-5? | * Yes | * No |
| 6 | Is the agency security plan supported by relevant policies, procedures and awareness? | * Yes | * No |
| 7 | Has a security threat and risk assessment been conducted for the agency? | * Yes | * No |
| 8 | Has the agency developed a risk register? | * Yes | * No |
| 9 | Has the agency risk tolerance been determined and documented? | * Yes | * No |
| 10 | Is the agency risk register prioritised according to agency criticality and risk tolerance? | * Yes | * No |
| 11 | Has the agency begun applying mitigations and treatments according to prioritised risks? | * Yes | * No |
| 12 | Does the agency regularly review and update the items listed 5-11? | * Yes | * No |
| 13 | Do agency security staff meet regularly to share information and coordinate approaches to agency security risks? | * Yes | * No |
| 14 | Has the agency developed reporting mechanisms for security incidents and breaches? | * Yes | * No |
| 15 | Do agency staff know how to report security concerns? Has this been validated? | * Yes | * No |
| 16 | Is there security awareness training and information readily available for all staff? | * Yes | * No |
| 17 | Are regular agency security performance assessments conducted? | * Yes | * No |
| 18 | Has business continuity been developed for the core functions of your agency? | * Yes | * No |
| 19 | Do the agency security staff have access to ASIO Outreach? | * Yes | * No |

Agency assessed security governance status:

Agency proposed measures to strengthen security governance status:

|  |  |
| --- | --- |
| Icon  Description automatically generated | Information Security |

|  |  |  |  |
| --- | --- | --- | --- |
| **Information Security** | | | |
| 1 | Does the agency have policies that clearly define expected information handling, processing, storage and management? | * Yes | * No |
| 2 | Are agency staff made aware of the above policies and guidelines, and are they provided refresher details at regular intervals (as necessary)? | * Yes | * No |
| 3 | Does the agency apply appropriate access controls to information and records systems? | * Yes | * No |
| 4 | Are the access controls and logs regularly reviewed and/or audited? | * Yes | * No |
| 5 | Does the agency comply with information classification requirements and legal obligations relating to information handling, processing, storage and management? | * Yes | * No |
| 6 | Do the agency security measures adequately protect all information management processes, ICT and other operational information systems (with the aggregate value of agency held information considered)? | * Yes | * No |
| 7 | Has the agency established practices and procedures that ensure security-classified information is only accessible and disseminated to those with suitably rated security clearances? | * Yes | * No |
| 8 | Are there established practices and procedures in place for the storage and destruction of security-classified information? | * Yes | * No |
| 9 | Does the agency have a clear desk policy? | * Yes | * No |
| 10 | Are the agency technology and information assets safeguarded during all stages of the asset lifecycle? | * Yes | * No |
| 11 | Does the agency have business continuity plans that ensure access to information is not hindered when required? | * Yes | * No |
| 12 | Does the agency have procedures for cyber breaches and are these reported to the Australian Cyber Security Centre (ACSC)? | * Yes | * No |
| 13 | Does the agency monitor open-source information that exists relating to their business, sites, functionality and development? Is this routinely refreshed? | * Yes | * No |
| 14 | Is there a ‘lock up’ policy for areas with substantial information and is this reviewed or exercised? | * Yes | * No |

Agency assessed information security status:

Agency proposed measures to strengthen information security status:

|  |  |
| --- | --- |
| Icon  Description automatically generated | People Security |

|  |  |  |  |
| --- | --- | --- | --- |
| **People Security** | | | |
| 1 | Does the agency conduct pre-employment screens and checks on all people who will have access to government-held information and resources? | * Yes | * No |
| 2 | Does the agency have processes in place to assess the ongoing suitability of all people who have access to government-held information and resources? | * Yes | * No |
| 3 | Does the agency have an established process for managing staff with security clearances? Does this include ensuring only those who require clearances are sponsored? | * Yes | * No |
| 4 | Is there a classified register containing the details of all people within the agency who have been sponsored with security clearances? Is this register regularly updated prompting review of clearances? | * Yes | * No |
| 5 | Are agency ‘Statement of Duties’ revised regularly, ensuring protective security is considered – with inclusion of relevant pre-employment screens or security clearances? | * Yes | * No |
| 6 | Does the agency provide the necessary briefing to staff with security clearances, including their responsibilities and associated expectations? | * Yes | * No |
| 7 | Do staff with security clearances receive travel briefings when they are travelling for both work and personal reasons e.g. awareness of political environment, managing approaches from adversaries, travelling with devices, etc? | * Yes | * No |
| 8 | Has the agency implemented annual staff performance, monitoring and reporting systems? Do these systems include security performance and assessment? | * Yes | * No |
| 9 | Has the agency adopted reporting protocols which ensure employment related disciplinary matters are referenced in personal security records and performance? | * Yes | * No |
| 10 | Do agency staff know how to identify and report suspicious, unusual, persistent or ongoing security concerns, breaches or incidents? | * Yes | * No |
| 11 | Does the agency conduct debrief and exit interviews for staff with security clearances? | * Yes | * No |
| 12 | Does the agency have visitor protocols which protect government information and confidentiality? | * Yes | * No |
| 13 | Is there a visitor escort policy, particularly in sensitive areas? | * Yes | * No |
| 14 | Does the agency provide security awareness training that supports policies and procedures? | * Yes | * No |

Agency assessed people security status:

Agency proposed measures to strengthen people security status:

|  |  |
| --- | --- |
| Icon  Description automatically generated | Physical Security |

|  |  |  |  |
| --- | --- | --- | --- |
| **Physical Security** | | | |
| 1 | Does the agency have clearly communicated policies that meet the TAS-PSPF requirements relating to physical security? | * Yes | * No |
| 2 | Does the agency have proportionate physical security applied to prioritised functions and assets (e.g. swipe card access, keys, locks, alarm systems, CCTV)? | * Yes | * No |
| 3 | Are physical access controls regularly reviewed (e.g. remove swipe access from those who transfer or retire, maintain up-to-date registers)? | * Yes | * No |
| 4 | Are the agency’s secure and/or restricted areas only accessible by staff with a suitable security clearance? | * Yes | * No |
| 5 | Are locks and storage devices appropriate for the classification level of the stored information? | * Yes | * No |
| 6 | Does the agency ensure any purchased and installed intruder detection systems and alarms are approved, maintained and tested? | * Yes | * No |
| 7 | Are both passive and active physical security measures tested and exercised for efficiency and improvement opportunities? | * Yes | * No |
| 8 | Does the agency restrict the use of electronic devices on a ‘needs’ basis? | * Yes | * No |
| 9 | Are the agency’s physical security measures consistent with relevant statutory requirements e.g. the *Work, Health and Safety Act 2012*? | * Yes | * No |
| 10 | Is the agency able to regulate the risk of technology, information and ICT assets being made inoperable or inaccessible, or being accessed without proper authorisation? | * Yes | * No |
| 11 | Has the agency developed plans and procedures to move to heightened levels of security in case of emergencies and increased threats? | * Yes | * No |
| 12 | Does the agency have appropriate security features in place to ensure the physical wellbeing of staff and visitors? | * Yes | * No |
| 13 | Does the agency consider and adopt environmental design as passive physical security when selecting or modifying facilities? | * Yes | * No |

Agency assessed physical security status:

Agency proposed measures to strengthen physical security status:

# Overall agency protective security

Through the answers provided above, consider the current agency protective security preparedness and resilience. This is an opportunity to enhance performance against the TAS-PSPF core requirements, in support of agency security scoping and planning.

A negative response to the answers in this document may not indicate an adverse result, remembering protective security mitigations ought to be proportionate to the assessed risk.

Point in time assessment of the agency’s protective security posture:

Any identified measures to enhance the agency’s protective security posture: