TAS-PSPF Tasmania's Protective Security Policy Framework

Information Security

INFOSEC-2:
Protecting official information

Department of Premier and Cabinet

Tasmanian Government

Contents

Author: Resilience and Recovery Tasmania
Publisher: Department of Premier and Cabinet
Date: April 2023

About this document

This document – INFOSEC-2: Protecting official information – is part of a suite of policies and guidance developed to assist Tasmanian Government agencies to meet requirements under Tasmania's Protective Security Policy Framework (TAS-PSPF).

The TAS-PSPF is a whole-of-government approach to the protection of Tasmanian Government information, people and assets from compromise and harm. It establishes minimum protective security standards and makes clear that to continue ensuring the security of our people and assets, Tasmanian Government agencies need to:

- understand the security environment in which they operate
- identify and understand the most critical assets they must protect
- mitigate security vulnerabilities on a prioritised security-risk basis
- anticipate and prepare for emerging security trends which threaten their ability to effectively undertake government business functions
- continue to improve protective security practices through accountability and governance.

The TAS-PSF sets out 14 core requirements – with each accompanied by supplementary requirements – that define what must be addressed in order to protect our information, people and assets.

The suite of policies and guidance, including those found in this document, ensures that the TAS-PSPF will be applied across Tasmanian Government agencies in a consistent way. It will also assist agencies to achieve the expected outcomes of the following protective security domains under the TAS-PSPF:

- security governance
- information security
- people security
- physical security.

The table below lists all 14 core requirements of the TAS-PSPF and their corresponding policies. The name of the policy and guidance provided in this document is highlighted.

Protective security outcome	Core requirement	Relevant policies and guidance
Security governance	1	GOVSEC-1: Establish security governance
	2	GOVSEC-2: Security advice and responsibilities
	3	GOVSEC-3: Security awareness
	4	GOVSEC-4: Annual reporting
	5	GOVSEC-5: Security planning
	6	GOVSEC-6: Reporting incidents and security investigations
Information security	7	INFOSEC-1: Access to, and management of, official information
	8	INFOSEC-2: Protecting official information
	9	INFOSEC-3: Robust technology and information systems
People security	10	PESEC-1: Recruiting the right people
	11	PESEC-2: Ongoing suitability assessment
	12	PESEC-3: Managing separating people
Physical security	13	PHYSEC-1: Protecting assets
	14	PHYSEC-2: Agency facilities

Definitions and shortened terms

Guiding term	What this means in the context of the TAS-PSPF
must/will/required/ responsible for	Any of these terms refer to an essential action that all agencies and Accountable Authorities must take.
must not	This term refers to an action that is prohibited – agencies and Accountable Authorities must NOT take this action.
should/ recommended	Either of these terms refer to an action that agencies and Accountable Authorities ought to take as best practice, unless justifiable circumstances exist.
should not	This term refers to an action that agencies and Accountable Authorities ought to avoid, unless justifiable circumstances prevent an alternative action.
may	This term refers to an action that is optional to agencies and Accountable Authorities.

Term	What this means in the context of the TAS-PSPF
Accountable Authority/ies	The person or people responsible for, and with control over, a Tasmanian Government public authority. This includes, but is not limited to, agencies (as defined in the *State Service Act 2000*), administrative units, bodies corporate, statutory authorities, and instrumentalities of the Crown.
agency/ies	A Tasmanian Government agency/department or sub-entity.
Agency Security Advisor	The person nominated to perform security functions or specialist services related to security within an agency. This role supports the Accountable Authority in security monitoring and compliance.
ASIO Outreach	ASIO's public-facing website, which provides advice to government, industry and academia on current and emerging security threats and security policy, available by subscription.
asset	An agency's people, information, and physical items, including ICT systems, technology and information infrastructure.
availability	Ensuring that authorised users have access to information and associated assets when required.
classification	A process that determines and stipulates the extent of protection required to prevent information from compromise and harm.

Term	What this means in the context of the TAS-PSPF
compromise	May include exposure to loss and unintended or unauthorised access, misuse, information disclosure and intrusion of business activities and information. Compromise is a risk and hindrance to business delivery, safety and security.
confidentiality	Ensuring that information is accessible only to those authorised to have access and a 'need to know'.
consequence	The outcome, or expected outcome, of any compromise of information or a security incident.
contractor	External or third party contracted to provide services to an agency. For the purpose of the TAS-PSPF, contractor includes sub-contractor and service provider.
core requirement	A requirement that agencies must meet to achieve the government's required protective security outcomes. Each of the 14 TAS-PSPF policies includes a core requirement (as well as supplementary requirements).
employees	All people conducting work on an agency premises, including contractors. See also, people.
function	The purpose or role of an agency.
handling	Any processes for accessing, transmitting, transferring, storing or disposing of official information.
integrity	Safeguarding the accuracy and completeness of information and processing methods, i.e. information has been created, modified or deleted by the intended authorised means and is correct and valid.
official information	All Tasmanian Government documents, intellectual property and information that is held, transmitted, or obtained by an agency.
originator	The instigating individual (or agency) who generated or received the information and is responsible for classifying it.
outcomes	The protective security 'end-state' aims of the Tasmanian Government relating to 4 security domains: governance, information, people and physical.
people	Employees and contractors, including secondees and any service providers that an agency engages. It also includes anyone who is given access to Tasmanian Government assets.
principles	Fundamental values that guide decision-making. There are 5 principles that inform protective security settings in the TAS-PSPF. 1. Security is a responsibility of government, its agencies and its people.

Term	What this means in the context of the TAS-PSPF
	2. Each agency is accountable and owns its security risks. 3. Security will be guided by a risk management approach. 4. Strong governance ensures protective security is reflected in agency planning. 5. A positive security culture is critical.
protection	The processes and procedures applied to ensure the confidentiality, integrity and availability of information and assets.
protective marking	The level of classification applied to information, and any other handling instructions or protections the information requires due to the level of harm should it be compromised.
PSPF maturity rating	The level to which an agency has addressed and implemented the core and supplementary requirements in the TAS-PSPF.
Responsible Executive	The person who oversees protective security matters within your agency, they may also be the Chief Security Officer (CSO).
risk appetite	The risk an agency or Accountable Authority is willing to accept.
risk tolerance	The level of risk an agency is comfortable taking after risk treatments have been applied to achieve an objective or manage a security risk.
security classified	Information that holds a classification of PROTECTED, SECRET or TOP SECRET and must be protected against compromise. Access to the information must be controlled and accessed by appropriately security cleared people.
security culture	The characteristics, attitudes and habits within an organisation that establish and maintain security.
security incident	A security incident is: • an action, whether deliberate, reckless, negligent or accidental, that fails to meet protective security requirements or agency-specific protective security practices and procedures which results, or may result in, the loss, damage, corruption or disclosure of information or assets • an approach from anybody seeking unauthorised access to protected assets • an observable occurrence or event (including natural or man-made events) that could harm Tasmanian Government information, people or assets.
security maturity	The measure of an agency's ability to manage their security risks within their risk environment and aligned to their risk tolerances.

Term	What this means in the context of the TAS-PSPF
security plan	Central document detailing how an agency plans to manage and address their security risks.
security risk	Something that could result in compromise, loss, unavailability or damage to information or assets, or cause harm to people.
security risk management	Managing risks related to an agency's information, people and assets.
security vetting	An authorised vetting agency's assessment of a clearance subject's suitability to hold a security clearance.
sensitive	Information classified as sensitive is not security-classified information; however, this information requires some protections on a 'needs to know' basis.
supplementary requirements	The actions needed to implement the TAS-PSPF core requirements and attain the government's required protective security outcomes. Each of the 14 core requirements includes supplementary requirements to help implement the TAS-PSPF.
threat	The intent and capability of an adversary.
threat actor/adversary	An entity that is partially or wholly responsible for an incident that impacts – or has the potential to impact – an agency's security.
visitor	Any person who attends an agency and/or has access to its assets, who is not employed or otherwise engaged by that agency.
zone	The physical locality, workspaces, and design of areas within an agency that store assets and information, specifically where information is produced, accessed, handled and stored. Security zoned areas range from 1-5, where the security requirements increase with the applicable zone number allocation.

Acronym/abbreviation	Meaning
ASA	Agency Security Advisor
ASD	Australian Signals Directorate
ASIO	Australian Security Intelligence Organisation
CDR	classified document register
COI	community of interest
DPAC	Department of Premier and Cabinet
DFAT	Department of Foreign Affairs and Trade
IMMs	information management markers
MoG	Machinery of Government
RDS	Retention and Disposal Schedules
RGB model	Red, Green, Blue model (when applying protective markings)
SCEC	Security Construction and Equipment Committee
SEEPL	Security Equipment Evaluated Product List

Context

The **INFOSEC-2: Protecting official information** policy and guidance will assist agencies to achieve an effective protective security outcome within the information security domain of the TAS-PSPF. They address core requirement 8 and its supplementary requirements.

Core requirement 8

Agencies will adopt the Australian Government's Protective Security Policy Framework and related documentation for the classification, protective marking, transfer, handling and storage requirements of information (in any format) relative to its value, importance and sensitivity.

Supplementary requirements

To achieve the standards required relating to the classification, protective marking, transfer, handling and storage requirements of information, the Accountable Authority will:

a) implement processes that ensure information is assessed, marked and managed in alignment with policies and protocols or the assigned security classification

b) provide and regularly promote awareness of information protection practices, including secure information sharing and handling expectations, along with privacy obligations

c) determine appropriate information classification based on assessment of the information and/or technology assets holding that information, applying relevant controls, protections, processes, and handling standards

d) when assessing sensitivity and security, the classification should be set at the lowest reasonable level to protect its confidentiality, integrity or availability from compromise or harm

e) ensure all information (including emails) is clearly identified with the correct protective markings[1]

f) adopt the Tasmanian Information and Records Management Standard, particularly in the creation of metadata, when records are created or captured, and ensure metadata reflects any protective markings[2]

[1] According to the assessed value and business impact of any compromise to the information as determined necessary.

[2] For access to the Tasmanian Information and Records Management Standard, refer to the website of the Office of the State Archivist at https://osa.tas.gov.au/wp-content/uploads/2023/08/Information-and-Records-Management-Standard.pdf.

g) when transferring, migrating or transmitting sensitive or security-classified information, ensure adequate processes exist to deter and detect any form of compromise to that information

h) manage and report breaches or security incidents to the Agency Security Advisor (ASA)[3]

i) comply with storage requirements for sensitive and security-classified information, ensuring appropriate secure containers and zones are applied as necessary

j) ensure compliance with secure disposal of sensitive and security-classified information.

Agencies have varied operating environments and associated risks which influence agency risk appetite and tolerance. The TAS-PSPF states agencies must apply protections to information, based on assessed value and business impact levels to ensure consistent application.

Accountable Authorities should consider the value of their information as an aggregate when applying mitigations and upholding compliance with the TAS-PSPF.

[3] Types of breaches include, but are not limited to, information privacy and all data, cyber, electronic and physical information breaches/incidents.

Guidance

Introduction

Information security is a key component of your agency's protective security regime. This policy and guidance details how to appropriately assess the sensitivity or security classification of your agency's information and adopt marking, handling, storage, and disposal arrangements that guard against information compromise.

Official information refers to all information that is created, sent, or received as part of the work of the Tasmanian Government. This information is an official record, and it provides evidence of what an agency has done and why. It can be collected, used, stored, and transmitted in various ways, including electronic, physical, and verbal.

Information is a valuable asset, meaning that any compromise – accidental or deliberate – may have an adverse impact on your agency, another agency, the community or the Tasmanian Government. Therefore, protecting the confidentiality, integrity and availability of all information is crucial. All official information must be protected according to the assessed business impact that any compromise of the information could cause.

Information compromise may include:

- loss
- misuse
- interference
- unauthorised access
- unauthorised modification
- unauthorised disclosure.

Required action: Implement procedures to assess, mark and manage information

Sensitive and security-classified information

Determining the classification of information in the Tasmanian Government promotes responsible management of information, open and transparent government, and accountability. The originator of information (this could be your agency or an individual who created or received the information) must assess the sensitivity of that information and determine the classification based on the likely damage as a result of compromise to the information's confidentiality. Only the originator can change the sensitivity or security classification applied to its information. Upon determining the sensitivity of the information, it should be appropriately classified and protected.

This policy (INFOSEC-2) requires agencies to implement controls to protect information holdings in proportion to their value, importance and sensitivity. While there is a focus towards sensitive and security-classified information, all official information requires an appropriate degree of protection.

Effective protection of information requires the correct assessment, marking and management of that information, according to the assigned classification. For further information, refer to Annexure 1.

Procedures to support protection

To support protection of information, agencies are required to implement processes which ensure information is assessed, marked and managed according to the assigned classification. When developing procedures for your agency, consider limiting any access to sensitive or security-classified information according to a 'need to know' (i.e. for an operational or organisational requirement). This will address the risk of unauthorised access and associated damage.

Your agency's information security measures should be applied in accordance with your agency's security plan. This may require you to implement protections in particular ways according to your specific risk and operating environments. You may need to apply a higher level of protection to meet business needs or to address your agency's security risks.

When developing procedures to support the protection of information, you must consider how you will maintain the confidentiality, integrity and availability of that information, particularly in the case of compromise.

- Confidentiality – by limiting access to, and the distribution of, information to authorised individuals only.
- Integrity – by making sure that effective security measures are in place to ensure that information creation, access, amendments and deletion is only performed by authorised individuals by intended means.
- Availability – by allowing access to information by authorised people for authorised purposes, and ensuring appropriate procedures are in place to support this access when it is needed.

It is important to understand and assess your agency's risks in relation to access to information, along with consideration of the aggregate value of your agency's information. While some information may only be considered as sensitive on its own, when aggregated with other available information, the value and outcome of any compromise increases. Refer to Annexure 2 for questions you should consider when assessing risks to your agency's information.

The development and implementation of information security policies and procedures should support your agency's security plan and assist staff in understanding their responsibilities in the protection of information. Refer to Annexure 3 for example topics which may be covered in information security policies and procedures.

Applying protective markings

To provide protection to your agency's sensitive or security-classified information, you must use protective markings which indicate the information's classification and any additional handling requirements. Applying protective markings helps users (as a visual) and systems (e.g. your agency's email gateway) to control the distribution of information.

The originator of any information is responsible for assessing and applying a classification; therefore, the originator must then apply the relevant protective markings to the information.

For more information, refer to the section **Protective markings** in this guidance document.

Applying caveats and accountable material

Caveats are applied to information, as a warning, in addition to an appropriate security classification, where special protections are required above those indicated by the classification. Caveats are not a standalone classification and must only be used in connection with a classification protective marking.

For more information, refer to the section **Protective markings** in this guidance document.

Limiting access

The TAS-PSPF policy: Access to, and management of, official information (INFOSEC-1) requires the 'need to know' principle to be applied to all access of sensitive and security-classified information. Limiting access on a 'need to know' basis guards against the risk of unauthorised access or misuse of information.

Records of disclosure and access

Monitoring and auditing your agency's access to, and dissemination of, information plays an important role in the protection of information. Highly classified information or caveated information (such as TOP SECRET information or accountable material[4]) must be recorded in an auditable register e.g. a Classified Document Register (CDR) or electronic document management system or repository. This register should be audited, with regular spot checks, and must document all incoming and outgoing information and material and transfers or copying of that material.[5]

Required action: Promote awareness of information protection practices

The Accountable Authority is responsible for ensuring their people are aware of information protection practices, implemented both from this policy and any agency-specific policies. This includes practices pertaining to secure information sharing and handling expectations, along with privacy obligations.

Privacy obligations

There are legislative requirements which apply to certain official information, impacting the parameters surrounding disclosure, use and handling. Under Section 3 of the *Personal Information Protection Act 2004* a 'personal information custodian' is defined as:

- a public authority[6]
- any body, organisation or person who has entered into a personal information contract relating to personal information
- a prescribed body.

[4] Accountable material is information requiring the strictest control over its access and movement.

[5] Should your agency be a participant in a national community of interest (COI), the relevant COI manual/practices/procedures will stipulate any additional requirements for information handling.

[6] As defined under the *Right to Information Act 2009*.

Tasmanian Government agencies are public authorities and, as such, must comply with the Personal Information Protection Principles, under Schedule 1 of the *Personal Information Protection Act 2004*. Agencies must ensure their people are aware of any responsibilities under the *Personal Information Protection Act 2004*, in addition to the requirements of this policy.

Sharing and handling of information

Your agency is required to promote information protection practices, including secure sharing and handling expectations. Sharing and handling sensitive and security-classified information must be in accordance with the protections required by the classification. Refer to Annexure 1 for information about minimum access protections.

Demonstrating good security practices and awareness when using sensitive and security-classified information can include:

- remaining vigilant and aware of the environment
- selecting work environments based on their suitability to use the required information
- taking all necessary steps to reduce the risk of unauthorised access, use or removal of information
- appropriate physical handling procedures when information is being carried or is not in active use.

Required action: Classify official information

Classifying information enables agencies to protect their information in a consistent, organised and appropriate way. The Tasmanian Government has elected to adopt the Australian Government's Protective Security Policy Framework in relation to the classification of information. The information below sets out the approved security classifications for use across the Tasmanian Government.

PROTECTED	This classification indicates compromise of the confidentiality of the information could be expected to cause damage to Tasmania's or the national interest, organisations, or individuals.
SECRET	This classification indicates compromise of the confidentiality of the information could be expected to cause serious damage to Tasmania's or the national interest, organisations, or individuals.
TOP SECRET	This classification indicates compromise of the confidentiality of the information could be expected to cause exceptionally grave damage to Tasmania's or the national interest, organisations, or individuals.

Table 1 – Security classifications

As demonstrated in the above table, the appropriate security classification is based on the probable damage resulting from compromise of the information's confidentiality. Where compromise of the information's confidentiality would cause limited damage and does not warrant one of the above security classifications, that information is considered sensitive and is treated as OFFICIAL: Sensitive.

All other information from your agency's business operations and services requires a routine level of protection and is treated as OFFICIAL. Any information that does not form part of official duties within your agency is treated as UNOFFICIAL. OFFICIAL: Sensitive, OFFICIAL and UNOFFICIAL are not deemed security classifications; however, they are protective markings.

It is important to note that any information which is sensitive or security-classified must be handled according to the requirements listed in Annexure 1, which includes the requirement for the user to be suitably security cleared and have a 'need to know'.

Proper use of security classifications

There are times when not all information contained within a document has the same classification. In these circumstances, it is important to note that the document must be classified in accordance with the most sensitive or security-classified information contained within.

As previously highlighted in this policy, the originator of the information must assess and assign the classification level, all protective markings, and any additional handling requirements. Using the BIL tool[7] (Annexure 4) to assist with determining a classification provides a mechanism to achieve consistency in the application of classifications across the Tasmanian Government.

It is important that your management of information enables your agency to meet business, government and community needs and expectations. You should balance the need to protect information with the need to ensure appropriate access.

Correctly limiting the quantity, scope, or time frame of sensitive and security-classified information achieves:

- the promotion of an open and transparent government
- accountability in government policies and practices that may be subject to inappropriate or over-classification
- external oversight of government operations and programs
- efficiency in managing information across government.

[7] This is a tool only and not intended to be proscriptive. However, using this tool will help you support the consistent assessment of the confidentiality, integrity and availability of information across the Tasmanian Government.

Security classifications should not be used to:

- restrain competition
- hide violations of law, inefficiency or administrative error to prevent embarrassment to an individual, organisation or agency
- prevent or delay the release of information which does not need protection.

When to assess information sensitivity or security classification

Agencies must assess the sensitivity or security classification of information when it is first created or received from external sources outside the Tasmanian Government. Doing this helps to protect the information at the earliest opportunity. Where there are significant changes, for example, a Machinery of Government (MoG) change, this also gives you the opportunity to reassess the sensitivity or security classification of information.

Sanitising, declassifying or reclassifying information

Where information may need to be shared to a broader audience, the originator may change the classification through editing, disguising or altering its content. To adequately address sanitisation, the following elements must be protected:

- Intelligence
- Sources
- Methods
- Capabilities
- Analytical procedures
- Privileged information

After sanitising the information, it may be declassified or reclassified at the discretion of the originator, who remains responsible for sanitising, declassifying or reclassifying the information.

Required action: Assign a level of security classification

The originator must set the classification at the lowest reasonable level to enable information to be accessed by the highest number of people with an identified 'need to know'. This requirement also helps to reduce over-classification of official information.

Over-classification of information can result in:

- access to official information being unnecessarily limited or delayed
- onerous administration and procedural overheads that add to costs
- classifications being devalued or ignored by staff and receiving parties.

The sensitivity or security classification can only be changed by the originator. If you consider that the application of a particular classification is inappropriate, you can query that original classification decision with the originator.

Required action: Apply correct protective markings

The originator must clearly identify sensitive and security-classified information by using the applicable protective markings.

Caveats and accountable material

There are 4 categories of caveats:

- sensitive compartmented information (codewords)
- foreign government markings
- special handling instructions
- releasability caveats.

Accountable material is information requiring the strictest control over its access and movement. Accountable material includes:

- TOP SECRET security-classified information
- some types of caveated information –
    - all codeword information
    - select special handling instruction caveats, particularly TAS CABINET information (see explanation in table below) at any security classification
- any classified information designated as accountable material by the originator.

What constitutes accountable material may vary from agency to agency;[8] however, each agency is responsible for and must handle caveated or accountable material in accordance with the originator's special handling requirements. You must not change caveats without approval from the originator.

[8] Accountable material may include budget papers, tender documents and sensitive ministerial briefing documents.

Caveat types	Caveat	The information covered	The special handling requirements imposed
Sensitive compartmented information (codewords)		Use of codewords is primarily within the national security community and the meaning is unrelated to the subject of the information. Each codeword indicates a special 'need to know' compartment. Compartments are the means to restrict access to information to set people who have been briefed on the particular sensitivities of the information and any special applicable rules.	The applicable special handling requirements will be specified by the agency that owns the information (the originating agency). If your agency receives any codeword caveats, you must contact the originating agency for guidance.
Foreign government markings		Foreign government markings are applied to information created by Australian agencies from foreign source information.	Your agency must safeguard foreign government-marked information to at least the equivalent of that required by the foreign government providing the information.
Special handling instructions	EXCLUSIVE FOR (named person)	The EXCLUSIVE FOR caveat identifies information intended for the specified recipient only.	You must limit access to EXCLUSIVE FOR information to a named person, position title or designation.
	TAS CABINET	The TAS CABINET caveat identifies information that: a) is prepared for the purpose of informing the Tasmanian Cabinet b) reveals decisions and/or deliberations of the Tasmanian Cabinet c) is prepared by agencies to brief their ministers on matters proposed for Tasmanian Cabinet decision-making.	You should only apply this caveat to information marked as OFFICIAL: Sensitive and above.

Caveat types	Caveat	The information covered	The special handling requirements imposed
	NATIONAL CABINET	The NATIONAL CABINET caveat identifies any information which has been prepared for National Cabinet or its subcommittees.	The Australian Government's Cabinet Handbook specifies handling requirements for Cabinet documents. You must handle information marked with the NATIONAL CABINET caveat in accordance with Cabinet conventions and within legal frameworks and processes such as Freedom of Information, parliamentary inquiries and judicial procedures. You should only apply this caveat to information marked as OFFICIAL: Sensitive and above.
Releasability caveats	Australian Eyes Only (AUSTEO)	The AUSTEO caveat indicates only appropriately cleared Australian citizens can access the information. Additional citizenships do not preclude access.	You must only pass – or allow access to – information marked as AUSTEO to Australian citizens. While a person holding dual citizenship may be given access to AUSTEO, in no instances may the Australian citizenship requirement be waived.
	Australian Government Access Only (AGAO)	The AGAO caveat indicates information that can only be accessed by appropriately cleared Australian citizens and appropriately cleared representatives of Five Eyes foreign governments on exchange, secondment, long-term posting or attachment within the National Intelligence Community and the Department of Defence.	Agencies which are not part of the National Intelligence Community and the Department of Defence must handle AGAO information as if it was marked AUSTEO.

Caveat types	Caveat	The information covered	The special handling requirements imposed
	Releasable To (REL)	The REL caveat identifies information that has been released or is releasable to the indicated foreign countries only.[9]	For example, REL AUS/CAN/GBR/NZL/USA means that the information may be passed to citizens of Australia, Canada, the United Kingdom, New Zealand and the United States of America only. This caveat is an exclusive marking that disqualifies a third-party national seconded or embedded in an Australian or foreign government agency from accessing the information.

Table 2 – Caveats and handling requirements

Information management markers

Information management markers (IMMs)[10] are optional markings your agency may apply to help manage the security of, and access to, information classified OFFICIAL: Sensitive or higher. These markers can help identify the type of content contained in the information.

The following IMMs are designated for use in Tasmania:

Legal privilege	Restrictions on access to, or use of, information covered by legal professional privilege.
Legislative secrecy	Restrictions on access to, or use of, information covered by specific legislative secrecy provisions. Apply with a warning notice which informs the recipient of relevant provisions.[11]
Personal privacy	Restrictions under the *Personal Information Protection Act 2004* on access to, or use of, personal information collected or received for business purposes.

[9] Countries are identified using 3-letter country codes from International Standard ISO 3166-1:2020 Codes for the representation of names of countries and their subdivisions – Alpha 3 codes.

[10] IMMs are not classifications and must only appear with an appropriate classification marking.

[11] Example of a warning notice –

> Legislative secrecy warning: Unless you have written consent from [insert authority or relevant position], it is an offence under section XX of the XXX Act to [insert details of restrictions].

Protective markings

The types of protective markings, and their order of precedence, are:

- classification
- foreign government information markings (if any)
- caveats or other special handling instructions (if any), then
- information management markers (optional, if any).

In addition to security classifications, the following protective markings may be applied.

- UNOFFICIAL – an optional marking that you may use to identify information generated for personal or non-work related purposes (some ICT systems may require you to apply this marking, e.g. email).
- OFFICIAL – identifying routine information produced or processed by the Tasmanian State Service. This marking indicates information which is not sensitive or security-classified and the marking is optional (some ICT systems may require you to apply this marking, e.g. email).
- OFFICIAL: Sensitive – a dissemination limiting marker (DLM). This marking indicates information which has been assessed as sensitive and requiring protection. When information is assessed at this level, the originator must apply this protective marking.

This policy (INFOSEC-2) does not recognise agency-specific and other protective markings. A standard set of markings ensures common understanding, consistency and interoperability across systems and government agencies. Creation of markings outside this policy may cause confusion about appropriate handling protections and increase the chance of compromise.

Text-based protective markings are the preferred method to identify sensitive or security-classified information and additional handling requirements.

Text-based protective markings should be:

- in capitals (other than for DLMs and IMMs), in a large plain font and a distinctive colour (red is preferred)
- centred and placed at the top and bottom of each page
- separated by a double forward slash (//) to help to clearly differentiate each marking.

For example:

OFFICIAL: Sensitive//Legal privilege

OFFICIAL: Sensitive//TAS CABINET

Paragraph grading indicators

Paragraph grading indicators identify the classification of individual paragraphs or sections within a document. You would use a paragraph grading indicator as an optional extra to the document's overall classification and protective markings.

If you do use paragraph grading indicators, the indicator should:

- appear in the same colour as the text of the document
- appear in brackets () at the start or end of each paragraph or in the margin adjacent to the first letter of the paragraph
- be written in full or abbreviated using the first letter/s of the markings –
    - UNOFFICIAL (U)
    - OFFICIAL (O)
    - OFFICIAL: Sensitive (O:S)
    - PROTECTED (P)
    - SECRET (S)
    - TOP SECRET (TS).

Applying protective markings in the absence of text-based markings

If you can't use text-based markings (e.g. certain media or assets), you must use colour-based markings for security-classified information. If using colour-based markings, use the RGB (Red, Green, Blue) model, as in the table below.[12]

Security classification	Colour-based marking	RGB cell colour
OFFICIAL: Sensitive[13]	Yellow	R 255, G 242, B 204
PROTECTED	Blue	R 79, G 129, B 189
SECRET	Salmon	R 229, G 184, B 183
TOP SECRET	Red	R 255, G 0, B 0

Table 3 – RGB colour-based markings

See Annexure I for information aligning each classification to its BIL, definition, protective marking, handling and access instructions.

Protective marking in emails

The preferred approach for marking emails is to apply the protective markings to the Internet Message Header Extension, consistent with the Australian Government's email protective marking standard,[14] which provides guidance on applying these markings.

Where an Internet Message Header Extension is not possible, place the protective markings in the subject field of an email.

Where an email with classification protective markings is printed, you must make sure that the markings are still visible.

[12] The RGB model is a manual colour selection function available in Word documents.

[13] A colour allocation is not a requirement; however, if colour is to be applied it must comply with the RGB configuration.

[14] Refer to the Australian Government's standard at www.protectivesecurity.gov.au/sites/default/files/2019-11/policy-8-annex-g-email-protective-marking-standard.pdf.

Required action: Create metadata

The Tasmanian Information and Records Management Standard describes the minimum requirements for managing information and records. It requires that you create metadata about records when they are created and/or captured. When you are considering the required protections of the record, metadata provides critical context and controls surrounding the access and use of information.

Protective marking in metadata

Within information on ICT systems, text-based protective markings are supplemented by metadata which assist to describe the security characteristics of the information or document.

From an information security perspective, the following metadata properties of importance are:

Security classification property	Identifies the security classification of the information and is used to identify information that is restricted to users with appropriate security clearance permissions. This property must be applied to all security-classified information.
Security caveat property	Can be used with the security classification property. This property indicates that the information requires additional special handling and that only people cleared and briefed to see it may have access. This property must be applied to all caveat information.
Rights property	This is an optional property to identify non-security related restrictions on the use of, or access, to records, e.g. IMMs. While this property is optional, if it is applied to information, the metadata must identify when it has been used.

Required action: Implement processes to protect information in transit

Under this policy (INFOSEC-2), agencies must ensure adequate processes exist to deter and detect any form of compromise to sensitive or security-classified information which is being transferred, migrated or transmitted.

When information is in transit, the risk of compromise increases, particularly if your agency does not have control over the entire network/s.

Examples of transferring information include:

- passing information to a person within an office environment (i.e. within your agency's facilities)
- sending information through your agency's internal mail to a person who works in the same building
- sending information through your agency's internal mail to a person who works in a different building
- handing or sending information to a person in another agency
- providing a person with a secure approved USB or other storage device that holds the information.

Examples of transmitting information include:

- emailing information to a person within your agency or in a different agency
- verbally communicating information to a person within your agency or another agency (e.g. by telephone or videoconference).

Examples of migrating information include when your agency:

- replaces or upgrades existing storage systems and equipment
- changes from local storage to cloud-based storage
- consolidates information systems.

If you are implementing processes to protect information in transit, start by ensuring that you apply the 'need to know' principle. You also need to ensure the appropriate security clearance of the recipient or security classification of the system that is performing migration.

Agencies must only transfer or transmit information for official purposes. When transferring or transmitting information for official purposes, you should identify recipients of sensitive and security-classified information by:

- a specific position, appointment or named individual
- a full location address (not a PO Box or similar)
- an alternate individual or appointment where relevant (e.g. for TOP SECRET information)
- where information is being electronically transmitted, an email address exclusive to those individuals with a 'need to know' (e.g. not a mailbox with unrestricted access).

The sensitivity or classification of information being transmitted or transferred should be obscured and a tamper-evident seal used to deter and detect unauthorised access. You can achieve this by:

- using appropriate encryption methods for transferring information over a public network or through unsecured spaces
- using double envelopes for physical information, i.e. by placing security-classified or accountable material inside 2 sealed envelopes. [15]

Use of devices to transfer or transmit information

Devices such as laptops, notebooks, tablets, mobile phones and USBs can be used to transfer and transmit information. Protecting sensitive and security-classified information that is being transferred or transmitted on these devices requires deterrence and detection from compromise.

Ways you can deter and detect information compromise and unauthorised access when devices are used include via password protection, multi-factor authentication, encryption of information at rest, and remote wiping capabilities.

Measures to control the transfer and transmission of information include the following.

- Receipts –
    - Receipts should identify the date and time of dispatch, the sender's name and a unique identifying number. Use receipts for transfer and transmission of all classified information.
    - When using receipts, keep an appropriate record of each handover of information (e.g. a 2-part receipt in the inner envelope with the sender's information, allowing the recipient to keep one portion and return the other to sender).
- Safe hand –
    - Safe hand refers to information which is dispatched to the recipient in the care of an authorised person who is responsible for the information's carriage and safe keeping.

[15] Double enveloping involves a) a tamper-evident inner envelope to detect unauthorised access and b) an outer envelope to obscure the information's sensitivity or classification and deter unauthorised access.

The outer envelope should not be marked with the classification or other protective markings.

The inner envelope can consist of an envelope or pouch sealed with a SCEC-approved tamper-evident seal so that any tampering is detected, or a SCEC-approved single-use envelope. The classification marking should be conspicuously placed on the inner envelope. Refer to the SCEC-approved SEEPL, via GovTEAMS, where users are required to register for an account and request access to the Protective Security community.

- Sending information using safe hand establishes an audit trail which provides confirmation that the recipient has received the information and helps to ensure the information is transferred in an authorised and secure facility or vehicle.
- To deter and detect any unauthorised access or information tampering, each handover of the information should include a receipt containing a unique identifying number, the time and date of the handover and the name and signature of the recipient.
- To send information using safe hand, you must –
  - assign a unique identification number (generally this will be the receipt number)
  - transfer the information in a security briefcase[16] or an approved mailbag[17]
  - not leave the information/item unattended.

- Safe hand via an endorsed courier –
  - There are various couriers endorsed by the Security Construction and Equipment Committee (SCEC) who are suitable to provide safe-hand courier services.[18]
  - In the instance of transferring valuable or attractive assets (e.g. pharmaceuticals or money), special arrangements may be required, such as armed escorts.
  - Special handling requirements may apply to caveated information, which may preclude the use of a safe-hand courier.

For further information about data migration, refer to Annexure 5 regarding minimum protections for information transfer or transit, and to TAS-PSPF policy: Robust technology and information systems (INFOSEC-3).

Required action: Manage and report security breaches and incidents

The TAS-PSPF outlines security breaches and incidents including, but not limited to, information privacy and all data, cyber, electronic and physical information breaches/incidents.

With this in mind, any suspected or actual compromise of classified information is considered a security incident. The TAS-PSPF policy: Security advice and responsibilities (GOVSEC-2) requires agencies to respond to, investigate and report on security incidents. In addition to this, agencies

[16] Refer to the SCEC's Security equipment guide of Briefcases for the carriage of security-classified information, via GovTEAMS, where users are required to register for an account and request access to the Protective Security Policy community.

[17] Refer to the SCEC-approved SEEPL via GovTEAMS for further information.

[18] ASIO T4 Protective security circular (PSC) 172.

must notify the owner or originator of the information as soon as practicable to the suspected or actual compromise.

It is recommended that you report any suspected or actual loss or compromise of SECRET or TOP SECRET information to the Department of Premier and Cabinet (DPAC) and the Australian Security Intelligence Organisation (ASIO).[19]

Required action: Comply with storage requirements

Sensitive and security-classified information must be stored securely to protect it from compromise. This also applies to mobile devices containing sensitive and security-classified information. Your agency must store information securely and preserve it, in an environment which prevents unauthorised access, duplication, alteration, removal or destruction.

The Australian Government Information Management Standard requires agencies to ensure their information assets are accessible for as long as needed and are shared appropriately, according to relevant access, security and privacy rules, within a protected and trusted environment. To effectively achieve this, your agency must implement information classification practices and protective marking procedures, recognising the protections the information requires.

The protections of information ought to be removed as soon as those protections are no longer required due to changes in the sensitivity or security classification. Refer to Annexure 6 for guidance on minimum use and storage requirements.

Clear desk, session and screen locking

It is recommended that agencies establish clear desk, session and screen locking procedures. These measures provide protection from compromise or harm to unattended information or resources. These measures involve your agency's people making sure that they:

- secure all hard-copy information
- lock any security containers as required
- not keep classified information on desks or in desk drawers
- lock device screens when not in use, or unattended.

[19] Contact DPAC via Resilience and Recovery Tasmania, requesting to speak with a member from the Office of Security and Emergency Management. Contact ASIO via their Outreach team (02) 6234 1668.

Required action: Securely dispose of sensitive and security-classified information

The creation of information does not mean it lasts forever; this is dependent on the nature of the information. Information is managed for as long as it has a business need or value – once it no longer has a business need or value, your agency may not need to keep it. When your agency's information is no longer required, you must archive, destroy, repurpose, or dispose of it in a secure manner.

Disposal of information includes the physical destruction of paper records, destruction of electronic records including deleting emails, documents or other data from business systems, transfer of records to another agency as a result of MoG changes and the transfer of records to a non-Tasmanian Government agency.

Under Section 20 of the *Archives Act 1983*, disposal and destruction of state records can occur under the requirement of law or with the written permission of the State Archivist, or in accordance with a practice or procedure approved in writing by the State Archivist. However, the Office of the State Archivist provides guidance on Retention and Disposal Schedules (RDS) which are a means to manage routine disposal without needing to seek authorisation from the State Archivist.[20]

Destroying sensitive or security-classified information

You can use various methods to securely destroy information, including:

- pulping
- burning
- pulverising – using a hammer mill
- disintegrating – by cutting and reducing the information particle size
- shredding – using crosscut shredders (standard strip shredders are not approved for the destruction of security-classified information).

Methods for destroying digital information include:

- digital file shredding
- degaussing by demagnetising magnetic media to erase recorded data

[20] Further information about RDS can be found on the website of the Office of the State Archivist at https://osa.tas.gov.au/retention-and-disposal.

- physical destruction of storage media through pulverisation, incineration or shredding[21]
- reformatting, if it can be guaranteed that the process cannot be reversed.

Commercial destruction services

Your agency may use commercial destruction services to destroy classified information. You should review the appropriateness of a commercial provider's collection process, transport, facility, procedures and approved equipment when considering engaging their destruction services. ASIO-T4 Protective Security Circular (PSC) 167 – Destruction of sensitive and security-classified information provides advice on engaging destruction services.[22]

The criteria for commercial destruction includes ensuring that:

- classified information is attended at all times and that vehicle and storage areas are appropriately secured
- destruction is performed immediately after the material has arrived at the premises
- destruction of classified information is witnessed by a representative from your agency
- destruction service staff have a security clearance to the highest level of security-classified information being transported and destroyed, or appropriately security cleared people from your agency escort and witness the destruction.

A number of commercial providers hold National Association for Information Destruction AAA certification for destruction services (with endorsements as specified in PSC 167 Destruction of security-classified information). These commercial providers are able to destroy security-classified information.[23]

It is recommended that information classified TOP SECRET or accountable material be destroyed within your agency's premises; the originating agency should request notification of destruction. The originator of some accountable material may apply special handling conditions that prevent information destruction being contracted out.

Refer to Annexure 7 for further information regarding the disposal of sensitive and security-classified information.

---

[21] Refer to the Australian Government Information Security Manual for guidance on sanitation and destruction of ICT equipment and storage media.

[22] Available via GovTEAMS, where users are required to register for an account and request access to the Protective Security Policy community.

[23] To search for destruction services which are NAID AAA certified with PSPF endorsement, please visit www.naidonline.org/naus/en/

Annexure 1 – Alignment of classifications to a business impact level (BIL), protective marking and access requirements

	Sensitive information		Security-classified information		
	OFFICIAL	**OFFICIAL: Sensitive**	**PROTECTED**	**SECRET**	**TOP SECRET**
BIL	**1 – Low**	**2 – Low to medium**	**3 – High**	**4 – Extreme**	**5 – Catastrophic**
Compromise of information would be expected to cause -	**Not applicable**. This is the majority of routine information created or processed by Tasmanian agencies.	**Limited damage** to an individual, organisation or government generally if compromised.	**Damage** to the state or national interest, organisations or individuals.	**Serious damage** to the state or national interest, organisations or individuals.	**Exceptionally grave damage** to the state or national interest, organisations or individuals.
Text-based marking	Mandatory OFFICIAL	Mandatory OFFICIAL: Sensitive	Mandatory PROTECTED	Mandatory SECRET	Mandatory TOP SECRET
If text-based markings cannot be used	Colour marking not required.	Colour marking not required.	Blue colour marking required.	Salmon colour marking required.	Red colour marking required.
'Need to know'	Not required, but recommended.	Yes	Yes	Yes	Yes
Valid security clearance	Not applicable. Effective employment screening is a sufficient security control.	Not applicable. Effective employment screening is a sufficient security control.	Yes Baseline	Yes Negative Vetting 1	Yes Negative Vetting 2 or above

Annexure 2 – Assessing risks to your agency's information: questions to consider

Question	Consideration
Where is your agency vulnerable?	Identify areas where your agency may be vulnerable to information security breaches, either accidental or intentional. How might these vulnerabilities be exploited and what measures can you apply to limit the risk of compromise and harm?
What threats does your agency face?	What are the potential threats to your agency's information security? Maintain contemporary knowledge of these threats. Who would benefit from having access to your agency's information, what would they use it for and what is they would want?
What impact would an information security breach have?	Assess and understand how your agency would be impacted in the event your information security is breached. What is the confidentiality, integrity and availability of your information?
Are supply chain risks considered?	Supply chains are increasing in complexity, have you considered each part of your agency's supply chain in your security risk assessment? Has your supplier verified their connections and dependencies?
Have the risks from collections of information been considered?	Any collections of information are considered as aggregated information. Aggregated information is typically more valuable than the singular pieces of information that together form the collection. In this situation, you should apply greater protections. What could be obtained from this collection if it were breached? Aggregated information relates to both physical and ICT collections.
Are your current security measures sufficient?	Consider your existing measures – will they adequately protect your information from the risks identified? If your information security was breached and/or any data stolen – could your agency determine what has been lost and could you recover it?

Annexure 3 – Information security policies and procedures: some example topics

Copying of information	Disposal of information
Electronic transfer of information	Handling of personal information
Home-based work security requirements	Management of information within the office
Management of outsourced services and functions	Safeguarding of government information
Use of security classifications	The ‘need to know’ principle
Physical transfer of information	Security container management
Storage of information	Electronic and removable media restrictions

Annexure 4 – Business impact levels (BIL) tool

	Sensitive information		Security-classified information		
	OFFICIAL	**OFFICIAL: Sensitive**	**PROTECTED**	**SECRET**	**TOP SECRET**
BIL	**1 – Low**	**2 – Low to medium**	**3 – High**	**4 – Extreme**	**5 – Catastrophic**
What the compromise of information would be expected to cause	Compromise of OFFICIAL information would result in **no or insignificant damage to individuals, organisations or government** – the majority of official information created or processed by Tasmanian agencies. This includes routine business operations and services.	Compromise of OFFICIAL: Sensitive information would result in **limited damage to an individual, organisation or government.** OFFICIAL: Sensitive information is that which requires limited dissemination. This is not a security classification; rather a dissemination limiting marker (DLM).	Compromise of PROTECTED information would be expected to cause **damage to the state or the national interest, organisations or individuals.** This information is valuable, important and sensitive.	Compromise of SECRET information would be expected to cause **serious damage to the state or the national interest, organisations or individuals.** This information is very valuable, important and sensitive.	Compromise of TOP SECRET information would be expected to cause **exceptionally grave damage to the state or the national interest, organisations or individuals.** This information is the most valuable, important and sensitive.

Potential impact on individuals from compromise of the information					
	Sensitive information		Security-classified information		
	OFFICIAL	**OFFICIAL: Sensitive**	**PROTECTED**	**SECRET**	**TOP SECRET**
BIL	**1 – Low**	**2 – Low to medium**	**3 – High**	**4 – Extreme**	**5 – Catastrophic**
Dignity or safety of an individual (or those associated with the individual)	Information from routine business operations and services. Includes personal information as defined in the *Personal Information Protection Act 2004*.[24]	Limited damage to an individual is the compromise of personal information leading to – a) potential harm, e.g. injuries that are not serious or life threatening b) discrimination, mistreatment, humiliation or undermining an individual's dignity or safety that is **not life threatening.**	Damage to an individual is discrimination, mistreatment, humiliation or undermining of an individual's dignity or safety that leads to potentially **significant harm or potentially life-threatening injury.**	Serious damage is discrimination, mistreatment, humiliation or undermining people's dignity or safety that could reasonably be expected to **directly threaten or lead to the loss of life of an individual or small group.**	Exceptionally grave damage is: a) widespread loss of life b) discrimination, mistreatment, humiliation or undermining people's dignity or safety that could reasonably be expected to directly lead to the death of a large number of people.

[24] Under the *Personal Information Protection Act 2004*, personal information is defined as: any information or opinion in any recorded format about an individual –
a) whose identity is apparent or is reasonably ascertainable from the information or opinion; and
b) who is alive or has not been dead for more than 25 years.

Potential impact on organisations from compromise of the information					
	Sensitive information		**Security-classified information**		
	OFFICIAL	**OFFICIAL: Sensitive**	**PROTECTED**	**SECRET**	**TOP SECRET**
Agency operations, capability and service delivery	Information from routine business operations and services.	Limited damage to agency operations is: a) a degradation in organisational capability to an extent and duration that, **while the agency can perform its primary functions,** the effectiveness of the functions is noticeably reduced b) minor loss of confidence in government.	Damage to agency operations is: a) a degradation in, or loss of, organisational capability to an extent and duration that the **agency cannot perform one or more of its primary functions** b) major loss of confidence in government.	Serious damage to agency operations is: a) a severe degradation in, or loss of, organisational capability to an extent and duration that the **agency cannot perform any of its functions** b) directly threatening the internal stability of Australia.	Not applicable. Impacts on an agency or organisation due to compromise of information at this scale are considered a matter of state or national interest.
Agency assets and finances e.g. operating budget	Information compromise would result in insignificant impact to the agency assets or annual operating budget.	Information compromise would result in limited damage to agency assets or the annual operating budget**.**	Damage is: a) substantial financial loss to an agency b) substantial damage to agency assets	Not applicable. Impacts on an agency or organisation due to compromise of information at this scale are considered a matter of state or national interest.	Not applicable. Impacts on an agency or organisation due to compromise of information at this scale are considered a matter of state or national interest.

Legal compliance	Information compromise would not result in legal and compliance issues.	Limited damage is: a) issues of legal professional privilege for communications between legal practitioners and their clients b) contract or agreement non-compliance c) failure of statutory duty d) breaches of information disclosure limitations under legislation resulting in less than 2 years' imprisonment.	Damage is: a) failure of statutory duty or breaches of information disclosure limitations under legislation resulting in 2 or more years' imprisonment.	Not applicable. Impacts on an agency or organisation due to compromise of information at this scale are considered a matter of state or national interest.	Not applicable. Impacts on an agency or organisation due to compromise of information at this scale are considered a matter of state or national interest.
Aggregated data[25]	An aggregation of routine business information.	A significant aggregated holding of information that, if compromised, would cause limited damage to the state or national interest, organisations or individuals.	A significant aggregated holding of sensitive information that, if compromised, would cause damage to the state or the national interest, organisations or individuals.	A significant aggregated holding of sensitive or classified information that, if compromised, would cause serious damage to the state or the national interest, organisations or individuals.	A significant aggregated holding of sensitive or classified information that, if compromised, would cause exceptionally grave damage to the state or national interest, organisations or individuals.

[25] A compilation of information may be assessed as requiring a higher security classification where the compilation is significantly more valuable than its individual components. This is because the collated information reveals new and more sensitive information or intelligence than would be apparent from the main source records and would cause greater damage than individual documents. When viewed separately, the components of the information compilation retain their individual classifications.

Potential impact on the Tasmanian Government or national interest from compromise of the information					
	Sensitive information		**Security-classified information**		
	OFFICIAL	**OFFICIAL: Sensitive**	**PROTECTED**	**SECRET**	**TOP SECRET**
Policies and legislation	Information compromise from routine business operations and services. For example, this may include information in a draft format (not otherwise captured by higher BIL).	Limited damage to government is impeding the development or operation of policies.	Damage to the national interest is: a) impeding the development or operation of major policies b) revealing deliberations or decisions of Australian Government Cabinet, or matters submitted, or proposed to be submitted, to Australian Government Cabinet[26] (not otherwise captured by higher-level business impacts).	Serious damage to the national interest is a severe degradation in development or operation of multiple major policies to an extent and duration that the policies can no longer be delivered.	Exceptionally grave damage to the national interest is the collapse of internal political stability of Australia or friendly countries.

[26] This includes official records of Cabinet, Cabinet business lists, minutes, submissions, memoranda or matters without submission, and any other information that has been submitted or proposed to be submitted to Cabinet.

Economy	Information from routine business operations and services.	Limited damage is: a) undermining the financial viability of one or more individuals, minor state-based or owned organisations or companies b) disadvantaging a major state organisation or company.	Damage is: a) undermining the financial viability of a major state-based or owned organisation or company b) disadvantaging a number of major state organisations or companies c) short-term material impact on state or national finances or economy.	Serious damage to the national interest is: a) undermining the financial viability of an industry sector (multiple major organisations in the same sector) b) long-term damage to the state or national economy.	Exceptionally grave damage is the collapse of the state or national economy.
Infrastructure	Information from routine business operations and services.	Limited damage is damaging or disrupting state or territory infrastructure.	Damage is damaging or disrupting significant state or territory infrastructure.	Serious damage is shutting down or substantially disrupting significant national infrastructure.	Exceptionally grave is the collapse of all significant national infrastructure.
International relations	Information from routine business operations and diplomatic activities.	Limited damage is minor and incidental damage or disruption to diplomatic relations.	Damage is: a) short-term damage or disruption to diplomatic relations b) disadvantaging the state in international negotiations or strategy.	Serious damage is: a) severely disadvantaging the state in major international negotiations or strategy b) directly threatening internal stability of friendly countries, leading to widespread instability	Exceptionally grave damage is directly provoking international conflict or causing exceptionally grave damage to relations with friendly countries.

				c) raising international tension or severely disrupting diplomatic relations resulting in formal protest or sanction.	
Crime prevention, defence or intelligence operations	Information from routine business operations and services.	Limited damage is: a) impeding the detection, investigation, prosecution of, or facilitating the commission of low-level crime b) affecting the non-operational effectiveness of Australian or allied forces without causing risk to life.	Damage is: a) impeding the detection, investigation, prosecution of, or facilitating the commission of an offence with 2 or more years imprisonment b) affecting the non-operational effectiveness of Australian or allied forces that could result in risk to life.	Serious damage is: a) major long-term impairment to the ability to investigate or prosecute serious organised crime[27] affecting the operational effectiveness, security or intelligence capability of Australian or allied forces.	Exceptionally grave damage is significantly affecting the operational effectiveness, security or intelligence operations of Australian or allied forces.

[27] Serious organised crime as defined in the Convention Against Transnational Organised Crime; for more information, refer to www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html

Annexure 5 – Minimum protections for information transfer and transmission

	Sensitive information		Security-classified information		
	OFFICIAL	**OFFICIAL: Sensitive**	**PROTECTED**	**SECRET**	**TOP SECRET**
Business impact level (BIL)	**1 – Low**	**2 – Low to medium**	**3 – High**	**4 – Extreme**	**5 – Catastrophic**
Protect information when taken out of the office for official purposes	Yes, for official purposes.	Yes, for official purposes.	Yes, for official purposes, but secure information in personal custody in a security briefcase or SCEC-approved pouch.	Yes, for official purposes, but: a) subject to agency arrangements for managerial approval b) secure information in personal custody in a security briefcase or SCEC-approved pouch.	Yes, but not recommended: a) written, manager-approved record of outgoing material maintained in an auditable log or classified document register (CDR) b) secure information in personal custody in a security briefcase or SCEC-approved pouch.
Protect information when used for home-based work	Yes, for official purposes, but in line with agency policies. See Annexure 8 for minimum requirements.	Yes, for official purposes but: a) in line with agency policies b) secure information from unauthorised access. See Annexure 9 for minimum requirements.	Use and storage of information for home-based work is not recommended. See Annexure 10 for minimum requirements.	Use and storage of information for home-based work is not recommended. See Annexure 11 for minimum requirements.	Not applicable. Use and storage for home-based work is prohibited. See Annexure 12 for further details.

Protect information when transferred over public network infrastructure or through unsecured spaces	Yes, for official purposes but 'need to know' principle should be applied.	Yes, for official purposes but information must be encrypted for transfer over public networks or through Zone 1 security areas.[28]	Yes, for official purposes but information must be encrypted for transfer over public networks or through Zone 1 security areas.	Yes, for official purposes but information must be encrypted for transfer over public networks or through Zone 1 security areas.	Yes, for official purposes but must use High Assurance Cryptographic Equipment encryption for transfer over public networks or outside Zone 5 security areas.
Protect information when transferred within a single physical location (e.g. an office)	Yes, for official purposes but 'need to know' principle should be applied.	Yes, for official purposes but 'need to know' principle should be applied.	Yes, for official purposes but 'need to know' principle should be applied.	Yes, for official purposes but 'need to know' principle should be applied.	Yes, for official purposes but 'need to know' principle should be applied.
Protect information from unauthorised access when transferred between physical establishments in Australia	Yes, for official purposes but 'need to know' principle should be applied.	Yes, for official purposes but unauthorised access must be deterred, e.g. external mail is sealed.	Yes, for official purposes but: a) must be secured from unauthorised access b) double enveloping required if SCEC-endorsed courier used c) receipt required.	Yes, for official purposes but: a) must be secured from unauthorised access b) double enveloping and – i. a security briefcase (or SCEC-approved pouch) and delivered direct by an authorised person[29] or ii. SCEC-endorsed courier c) receipt required.	Yes, for official purposes but: a) must be secured from unauthorised access b) double enveloping and - i. a security briefcase (or SCEC-approved pouch) and delivered direct by an authorised person or ii. safe-hand courier c) receipt required.

[28] Encryption must be applied unless the residual risk of not doing so has been acknowledged and accepted by the agency.

[29] Authorised person is a person authorised in accordance with your agency's procedures to transfer sensitive and classified information which has been secured from unauthorised access. The authorised person may physically move the information between establishments within or outside Australia. As the information has been secured from unauthorised access, the authorised person does not require a security classification to the level of sensitive or security-classified information being transferred.

Protect information from unauthorised access when transferred between physical establishments outside Australia	Yes, for official purposes but 'need to know' principle should be applied.	Yes, for official purposes but unauthorised access must be deterred, e.g. external mail is sealed.	Yes, for official purposes but: a) double enveloping b) receipt required c) carriage by Department of Foreign Affairs and Trade (DFAT) courier service.	Yes, for official purposes but: a) double enveloping b) receipt required c) carriage by DFAT courier service.	Yes, for official purposes but: a) double enveloping b) receipt required c) carriage by DFAT courier service.

Annexure 6 – Minimum use and storage requirements for sensitive and security-classified information

	Sensitive information		Security-classified information		
	OFFICIAL	**OFFICIAL: Sensitive**	**PROTECTED**	**SECRET**	**TOP SECRET**
Business impact level (BIL)	**1 – Low**	**2 – Low to medium**	**3 – High**	**4 – Extreme**	**5 – Catastrophic**
Unattended zone or area	Apply a clear desk policy and screen protections.	Apply a clear desk policy and screen protections.	Apply a clear desk policy and screen protections.	Apply a clear desk policy and screen protections.	Apply a clear desk policy and screen protections.
Zone 1 **Public access**	Storage: Permitted if secured from unauthorised access, locked commercial container recommended. Use: Permitted.	Storage: Permitted if secured from unauthorised access, SCEC Class C container recommended. Use: Permitted.	Storage: Not to be stored unless unavoidable. If unavoidable, SCEC Class C container, commercial safe or vault. Use: Permitted.	Storage: Not to be stored. Use: Not to be used unless exceptional circumstances. Originating agency approval required.	Storage: Not to be stored. Use: Not to be used.
Zone 2 **Restricted public access.** **Unrestricted access for authorised personnel. May use single factor authentication for access control.**	Storage: Permitted if secured from unauthorised access. Use: Permitted.	Storage: Permitted if secured from unauthorised access. Use: Permitted.	Storage: Permitted if in SCEC Class C container. Use: Permitted.	Storage: Not to be stored unless exceptional circumstances. Originating agency approval required. SCEC Class A container. Use: Permitted.	Storage: Not to be stored. Use: Not to be used.

Zone 3 **No public access. Visitor access only for visitors with a need to know and close escort. Restricted access for authorised personnel. Single factor authentication for access control.**	Storage: Permitted if secured from unauthorised access. Use: Permitted.	Storage: Permitted if secured from unauthorised access. Use: Permitted.	Storage: Permitted if secured from unauthorised access, SCEC Class C container recommended. Use: Permitted.	Storage: Permitted if in SCEC Class B container. Use: Permitted.	Storage: Not to be stored unless exceptional circumstances: a) originating agency approval and ASIO-T4 advice required b) storage period up to 5 days in SCEC Class A container. Use: Permitted.
Zone 4 **No public access. Visitor access only for visitors with a 'need to know' and with close escort. Restricted access for authorised personnel with appropriate security clearance. Single factor authentication for access control.**	Storage: Permitted if secured from unauthorised access. Use: Permitted.	Storage: Permitted if secured from unauthorised access. Use: Permitted.	Storage: Permitted if secured from unauthorised access. Use: Permitted.	Storage: Permitted if in SCEC Class C container. Use: Permitted.	Storage: Not to be stored unless exceptional circumstances: a) originating agency approval and ASIO-T4 advice required b) storage period up to 5 days in SCEC Class A container. Use: Permitted.

Zone 5 **No public access. Visitor access only for visitors with a 'need to know' and with close escort. Restricted access for authorised personnel with appropriate security clearance. Dual factor authentication for access control.**	Storage: Permitted. Use: Permitted.	Storage: Permitted. Use: Permitted.	Storage: Permitted. Use: Permitted.	Storage: Permitted if in SCEC Class C container. Use: Permitted.	Storage: Permitted if in SCEC Class B container. Use: Permitted.

Annexure 7 – Minimum handling protections for disposal of sensitive and security-classified information, ICT and media equipment

	Sensitive information		Security-classified information		
	OFFICIAL	**OFFICIAL: Sensitive**	**PROTECTED**	**SECRET**	**TOP SECRET**
Destruction of physical information					
Use agency-assessed and approved (or National Association for Information Destruction AAA certified) destruction service with specific endorsement and approved equipment and systems	Not applicable. While all official information must be disposed of securely, there is no minimum requirement for how to dispose of OFFICIAL or OFFICIAL: Sensitive information.		Destroy information by pulping, burning, pulverisation, disintegration, or shredding (Class B crosscut shredder).	Destroy information by pulping, burning, pulverisation, disintegration, or shredding (Class A crosscut shredder).	Destroy information by pulping, burning, pulverisation, disintegration, or shredding (Class A crosscut shredder).
Destroyed under supervision of 2 officers cleared to the appropriate level who are to supervise the removal of the material to the point of destruction, ensure destruction is complete, and sign a destruction certificate	Not applicable. While all official information must be disposed of securely, there is no minimum requirement for how to dispose of OFFICIAL or OFFICIAL: Sensitive information.		Supervise and certify destruction of information if it is accountable material.	Supervise and certify destruction of information if it is accountable material.	Supervise and certify destruction of information.

Destruction of ICT and media equipment				
Undergo media sanitisation or destruction	Not applicable. While all official information must be disposed of securely, there is no minimum requirement for how to dispose of OFFICIAL or OFFICIAL: Sensitive information.	Sanitise or destroy ICT and media equipment.	Sanitise or destroy ICT and media equipment.	Sanitise or destroy ICT and media equipment.

Annexure 8 – Minimum protections and handling requirements for OFFICIAL information

Business impact level (BIL) 1	**OFFICIAL – No or insignificant damage to individuals, organisations or government**
Protective marking	Text-based marking for OFFICIAL documents (including emails) is optional. It is recommended that text markings are in capitals, bold, large fonts and a distinctive colour (red preferred). Markings should be placed at the top and bottom of each page. There is no requirement for colour-based marking of OFFICIAL information. For paragraph grading indicators, OFFICIAL should be written in full or abbreviated to (O) and placed at the start or end of the paragraph or in the margin adjacent to the first letter.
Access	'Need to know' principle should apply for OFFICIAL information. There is no security clearance requirement to access OFFICIAL information.
Use	OFFICIAL information can be used in security Zones 1-5 and outside agency facilities.
Storage	OFFICIAL information may be left unattended, subject to agency clear desk policies. It is recommended that mobile devices that process, store or communicate OFFICIAL information are secured if left unattended. Apply agency procedures for storage of OFFICIAL information. It is recommended that a lockable container is use in Zone 1 areas.
Carry	When carrying OFFICIAL information outside of agency facilities, apply agency procedures.
Transfer	When transferring OFFICIAL information, apply agency procedures for transfer by hand, internal mail or courier. For transfer outside agency facilities, it is recommended that opaque envelopes/folders are used to minimise risk of unauthorised access.
Transmit	It is recommended to encrypt OFFICIAL information for any communication that occurs over public network infrastructure, or through unsecured spaces (including Zone 1 areas).
Official travel	OFFICIAL information or mobile devices can be taken on domestic and overseas travel. Agency procedures should be applied, and environmental risks should be considered.
Disposal	OFFICIAL information should be destroyed securely.

Annexure 9 – Minimum protections and handling requirements for OFFICIAL: Sensitive information

Business impact level (BIL) 2	**OFFICIAL: Sensitive – Limited damage to individuals, organisations or government**
Protective marking	Text-based marking must be applied to OFFICIAL: Sensitive documents (including emails). It is recommended that text markings are in capitals, bold, large fonts and a distinctive colour (red preferred). Markings should be placed at the top and bottom of each page. If text-based markings cannot be used, colour-based markings may be used. The preferred colour for OFFICIAL: Sensitive is a yellow colour. For paragraph grading indicators, OFFICIAL: Sensitive should be written in full or abbreviated to (O:S) and placed at the start or end of the paragraph or in the margin adjacent to the first letter.
Access	The 'need to know' principle applies to all OFFICIAL: Sensitive information. There is no security clearance requirement to access OFFICIAL: Sensitive information; agency screening processes are sufficient.
Use	OFFICIAL: Sensitive information can be used in security Zones 1-5. For work outside agency facilities, including from home, external agency offices, cafes: a) apply agency procedures which may include conducting a security risk assessment of the proposed work environment b) exercise judgement to assess the environmental risk.
Storage	OFFICIAL: Sensitive information may be left unattended for short periods of time, subject to agency clear desk policies. It is recommended that all OFFICIAL: Sensitive information be stored securely when unattended. Mobile devices that process, store or communicate OFFICIAL: Sensitive information may be left unattended if in a secured state, e.g. password protected, encrypted. When storing OFFICIAL: Sensitive information inside agency facilities (Zones 1-5), store in a lockable container. When storing OFFICIAL: Sensitive information outside agency facilities (including at home): a) apply requirements for carrying outside agency facilities b) use of opaque envelopes/folders and/or lockable containers is recommended c) for regular, ongoing home-based work, an SCEC Class C container is recommended. When storing mobile devices which process, store or communicate OFFICIAL: Sensitive information inside agency facilities (Zones 1-5): if in a secured state, recommend storing in lockable container; if in an unsecured state, a lockable container must be used.

	Storage of mobile devices outside of agency facilities: a) apply requirements for carrying outside agency facilities b) apply agency procedures and exercise judgement to assess environmental risk c) if in a secured or unsecured state, recommend storage in a lockable container.
Carry	When carrying OFFICIAL: Sensitive information: a) inside agency facilities in Zones 1-5, an opaque envelope or folder is recommended. b) outside or between agency facilities, including for external meetings, an opaque envelope/folder is recommended. Mobile devices that process, store or communicate OFFICIAL: Sensitive information: a) inside agency facilities, in Zones 1-5, carry in a secured state. If unsecured, apply agency procedures. b) outside or between agency facilities, carry in a secured state. If unsecured, apply agency procedures.
Transfer	When transferring OFFICIAL: Sensitive information inside agency facilities: a) in Zones 1-5, an opaque envelope/folder is recommended b) transfer by hand. When transferring OFFICIAL: Sensitive information outside agency facilities to another facility: a) an opaque envelope/folder is recommended b) transfer by hand, agency safe hand, safe-hand courier c) tamper-evident packaging may be used.
Transmit	Electronic transmission of unencrypted OFFICIAL: Sensitive information must be over OFFICIAL secure networks (or higher). Encrypt OFFICIAL: Sensitive information for any communication that occurs over public network infrastructure, or through unsecured spaces (including Zone 1 areas), unless the risk of not doing so has been identified and accepted by the Accountable Authority.
Official travel	OFFICIAL: Sensitive information or mobile devices can be taken to external meetings and on domestic travel. When travelling domestically with OFFICIAL: Sensitive information (or mobile devices that process, store or communicate OFFICIAL: Sensitive information), apply agency procedures and exercise judgement to assess environmental risk. When travelling outside of Australia with OFFICIAL: Sensitive information: a) apply agency procedures and exercise judgement to assess environmental risk b) seek Department of Foreign Affairs and Trade (DFAT) advice on options to access information or devices at overseas destination. OFFICIAL: Sensitive information (or mobile devices) should not be left unattended while travelling; however, apply agency procedures and exercise judgement to assess environmental risk.
Disposal	OFFICIAL: Sensitive information must be destroyed securely.

Annexure 10 – Minimum protections and handling requirements for PROTECTED information

Business impact level (BIL) 3	PROTECTED – Damage to state or national interest, organisations or individuals
Protective marking	Text-based marking must be applied to PROTECTED documents (including emails). It is recommended that text markings are in capitals, bold, large fonts and a distinctive colour (red preferred). Markings should be placed at the top and bottom of each page. If text-based markings cannot be used, colour-based markings must be used. The preferred colour for PROTECTED is blue (RGB 79, 129, 189). For paragraph grading indicators, PROTECTED should be written in full or abbreviated to (P) and placed at the start or end of the paragraph or in the margin adjacent to the first letter.
Access	The 'need to know' principle applies to all PROTECTED information. Ongoing access to PROTECTED information requires a Baseline security clearance, or above. Temporary access to PROTECTED information must be supervised.
Use	PROTECTED information can be used in security Zones 1-5. Outside agency facilities (including at home): a) apply agency procedures, which must include conducting a security risk assessment of the proposed work environment b) for occasional home-based use, apply agency procedures and exercise judgement to assess the environmental risk. Use of PROTECTED information outside agency facilities or the home (e.g. external agency offices, cafés) is not recommended, but if necessary: a) apply agency procedures b) exercise judgement to assess the environmental risk.
Storage	PROTECTED information must not be left unattended. Information must be stored securely when unattended. Mobile devices that process, store or communicate PROTECTED information may be left unattended if in a secured state (e.g. password protected, encrypted). When storing PROTECTED information inside agency facilities (Zones 2-5 only): a) in Zones 4-5, store in a lockable container b) in Zones 2-3, store in a SCEC approved Class C container. It is not recommended to store PROTECTED information outside agency facilities (including at home), but if necessary: a) apply requirements for carrying outside agency facilities

	b) for regular, ongoing home-based work, install and store in a SCEC approved Class C or higher container c) for occasional home-based work, retain in personal custody (positive control), or for brief absences from home, apply agency procedures and exercise judgement to assess environmental risk d) return to agency facilities as soon as practicable. When storing mobile devices which process, store or communicate PROTECTED information inside agency facilities (Zones 1-5): a) in Zones 4-5, if in a secured state, recommend storing in lockable container; if in an unsecured state, you must use a lockable container b) in Zones 2-3, if in a secured state, recommend storing in a lockable container; if in an unsecured state, store in a SCEC approved Class C container c) in Zone 1, if in a secured state, store in a SCEC approved Class C container; if in an unsecured state, store in a higher security zone. Storage of mobile devices outside of agency facilities: a) apply requirements for carrying outside agency facilities b) apply agency procedures and exercise judgement to assess environmental risk c) if in a secured state, recommend storage in a lockable container; if in an unsecured state, store in a SCEC approved Class C container or higher.
Carry	When carrying PROTECTED information outside of agency facilities, information must be retained in personal custody (positive control) at all times. Inside agency facilities, in Zones 1-5, in an opaque envelope or folder that indicates classification. Outside or between agency facilities, including for external meetings, place in a security briefcase, pouch or satchel or recommended tamper-evident packaging.[30] Mobile devices that process, store or communicate PROTECTED information: Inside agency facilities – a) in Zones 2-5, if secured or unsecured, agency procedures are sufficient b) in Zone 1, carry in a secured state. Outside or between agency facilities, carry in a secured state; if in an unsecured state, carry inside a security briefcase, pouch or satchel and consider tamper-evident packaging.
Transfer	When transferring PROTECTED information inside agency facilities, in Zones 1-5, transfer by hand or agency safe hand, and apply all necessary handling requirements. Can be uncovered if transfer is in close proximity and there is a low risk of unauthorised viewing. When transferring PROTECTED information outside agency facilities to another facility –

[30] Refer to the SCEC-approved SEEPL via GovTEAMS for further information.

	a) apply requirements for carrying outside agency facilities b) transfer by hand, agency safe hand, safe-hand courier rated to BIL 4, or Department of Foreign Affairs and Trade (DFAT) courier (use tamper-evident packaging). A receipt of transfer must be obtained.
Transmit	Electronic transmission of unencrypted PROTECTED information must be over PROTECTED secure networks (or higher). Encrypt PROTECTED information for any communication that is not over a PROTECTED network (or higher).
Official travel	PROTECTED information or mobile devices can be taken to external meetings and on domestic travel. When travelling domestically with PROTECTED information (or mobile devices that process, store or communicated PROTECTED information): a) requirements for carrying outside agency facilities must be applied, including tamper-evident packaging b) information and/or device should be retained as carry-on baggage, but if not possible, try to observe entering and exiting the cargo hold and reclaim as soon as possible. PROTECTED information (or mobile devices) should not be left unattended while travelling domestically. For brief absences from a hotel room, apply agency procedures and exercise judgement to assess environmental risk. Travel outside of Australia with PROTECTED information is not recommended, but if necessary: a) seek DFAT advice on options to access information or devices at overseas destination b) apply agency procedures for carrying outside agency facilities c) information and/or device must be retained as carry-on baggage, and travel must not occur, if airline requires baggage to be checked d) do not leave PROTECTED information or devices unattended. Do not store while travelling (e.g. hotel safe). If storage is required, store in an Australian agency facility.
Disposal	PROTECTED information must be destroyed using a Class B shredder.

Annexure 11 – Minimum protections and handling requirements for SECRET information

Business impact level (BIL) 4	SECRET – Serious damage to state or national interests, organisations or individuals
Protective marking	Text-based marking must be applied to SECRET documents (including emails). It is recommended that text markings are in capitals, bold, large fonts and a distinctive colour (red preferred). Markings should be placed at the top and bottom of each page. If text-based markings cannot be used, colour-based markings must be used. The preferred colour for SECRET is salmon (pink) (RGB 229, 184, 183). For paragraph grading indicators, SECRET should be written in full or abbreviated to (S) and placed at the start or end of the paragraph or in the margin adjacent to the first letter.
Access	The 'need to know' principle applies to all SECRET information. Ongoing access to SECRET information requires a Negative Vetting 1 (NV1) security clearance, or above. Temporary access to SECRET information must be supervised.
Use	SECRET information can be used in security Zones 2-5. Outside agency facilities, SECRET information must not be used for regular or ongoing work. Home-based work is not recommended, but if necessary: a) written managerial approval must be obtained b) apply agency procedures and exercise judgement to assess environmental risk.
Storage	SECRET information (or mobile devices that process, store or communicate SECRET information) must not be left unattended. Information must be stored securely when unattended. When storing SECRET information inside agency facilities: a) in Zones 4-5, store in a SCEC approved Class C container b) in Zone 3, store in a SCEC approved Class B container. It is not recommended to store SECRET information outside agency facilities (including at home), but if necessary: a) apply requirements for carrying outside agency facilities b) retain in personal custody (positive control) or in a SCEC approved Class B (or higher) container for brief periods away from home that has been approved as a proper place of custody by the Accountable Authority or delegate c) return to agency facilities as soon as practicable.

	When storing mobile devices which process, store or communicate SECRET information inside agency facilities (Zones 2-5 only): a) in Zones 4-5, store in a SCEC approved Class C container b) in Zone 3, if in a secured state, store in a SCEC approved Class C container; if in an unsecured state, store in a SCEC approved Class B container c) in Zone 2, if in a secured state, store in a SCEC approved Class B container; if in an unsecured state, store in a higher security zone. Storage of mobile devices outside of agency facilities is not recommended, but if necessary (see use above): a) apply requirements for carrying outside agency facilities b) retain in personal custody (positive control), or in a SCEC approved Class C container that has been approved for use by the Accountable Authority or delegate.
Carry	When carrying SECRET information outside of agency facilities, information must be retained in personal custody (positive control) at all times. Inside agency facilities: a) in Zones 2-5, in an opaque envelope or folder that indicates classification b) in Zone 1, carry in an opaque envelope or folder that indicates classification and place in a security briefcase, pouch or satchel. Outside or between agency facilities, including for external meetings: a) place in a security briefcase, pouch or satchel b) recommended tamper-evident packaging. Mobile devices that process, store or communicate SECRET must remain in personal custody (positive control) at all times. Inside agency facilities: a) in Zone 5, if secured or unsecured, agency procedures are sufficient b) in Zones 2-4, carry in a secured state. If unsecured, apply agency procedures. c) in Zone 1, carry in a secured state; if in an unsecured state, place inside a security briefcase, pouch or satchel. Outside or between agency facilities, carry in a secured state; if in an unsecured state, carry inside a security briefcase, pouch or satchel and consider tamper-evident seals.
Transfer	When transferring SECRET information inside agency facilities, in Zones 1-5, transfer by hand or agency safe hand, and apply all necessary handling requirements. Can be uncovered if transfer is in close proximity and there is a low risk of unauthorised viewing. When transferring SECRET information outside agency facilities to another facility: a) apply requirements for carrying outside agency facilities b) transfer by hand, agency safe hand, safe-hand courier rated to BIL 4, or Department of Foreign Affairs and Trade (DFAT) courier (use tamper-evident packaging). A receipt of transfer must be obtained.

Transmit	Electronic transmission of unencrypted SECRET information must be over SECRET secure networks (or higher). Australian Signals Directorate (ASD)'s High Assurance Cryptographic Equipment[31] must be used to encrypt SECRET information for any communication that is not over a SECRET network (or higher).
Official travel	Travelling inside or outside of Australia with SECRET information or mobile devices is not recommended, but if necessary: a) requirements for carrying outside agency facilities must be applied, including tamper-evident packaging b) information and/or device must be retained as carry-on baggage, and travel must not occur if airline requires baggage to be checked. SECRET information must not be left unattended. Do not store while travelling (e.g. hotel room safes). If storage is required, it must be within an appropriate Australian agency facility. If access to SECRET information or mobile devices provided at overseas destination: a) seek DFAT advice on options to access information or devices at overseas destination b) requirements for carrying outside agency facilities must be applied c)) information and devices must be retained in personal custody (positive control) at all times or stored in an Australian agency's facilities.
Disposal	SECRET information must be destroyed using a Class A shredder.

[31] Refer to the Australian Cyber Security Centre website for further information Guidelines for Cryptography | Cyber.gov.au

Annexure 12 – Minimum protections and handling requirements for TOP SECRET information

Business impact level (BIL) 5	TOP SECRET – Exceptionally grave damage to the state or national interest, organisations or individuals
Protective marking	Text-based marking must be applied to TOP SECRET documents (including emails). It is recommended that text markings are in capitals, bold, large font and a distinctive colour (red preferred). Markings should be placed at the top and bottom of each page. If text-based markings cannot be used, colour-based markings must be used. The preferred colour for TOP SECRET is red (RGB 255,0,0). For paragraph grading indicators, TOP SECRET should be written in full or abbreviated to (TS) and placed at the start or end of the paragraph or in the margin adjacent to the first letter.
Access	The 'need to know' principle applies to all TOP SECRET information. Ongoing access to TOP SECRET information requires a Negative Vetting 2 (NV2) security clearance, or above. Temporary access to TOP SECRET information can only be given to people who hold at least a Negative Vetting 1 (NV1) security clearance, and use must be supervised.
Use	TOP SECRET information can only be used in security Zones 3-5. TOP SECRET information must not be used outside of agency facilities.
Storage	TOP SECRET information (or mobile devices that process, store or communicate TOP SECRET information) must not be left unattended. Information must be stored securely when unattended. When storing TOP SECRET information (or mobile device) inside agency facilities: a) in Zone 5, store in a SCEC approved Class B container b) in Zones 3-4, store in exceptional circumstances only and for a maximum of 5 days c) in Zone 4, store in a SCEC approved Class B container d) in Zone 3, store in a SCEC approved class A container. TOP SECRET information (or mobile devices) must not be stored outside agency facilities (including at home).
Carry	When carrying outside of agency facilities, TOP SECRET information must be retained in personal custody (positive control) at all times. Inside agency facilities: a) in Zones 3-5, in an opaque envelope or folder that indicates classification b) carrying in Zones 1-2 is not recommended, but if necessary, carry in an opaque envelope or folder that indicates classification and place in a security briefcase, pouch or satchel.

	Carrying outside or between agency facilities, including for external meetings, is not recommended, but if necessary: a) obtain written manager approval b) place in tamper-evident packaging within a security briefcase, pouch or satchel. Mobile devices that process, store or communicate TOP SECRET information require explicit approval by ASD. All devices must remain in personal custody (positive control). Inside agency facilities: a) in Zones 3-5, carry in secured state (e.g. locked, password protected) b) in Zones 1-2, carry in a secured state. If unsecured, place inside security briefcase, pouch or satchel. Carrying outside or between agency facilities, including for external meetings, is not recommended, but if necessary: a) obtain written manager approval b) place in tamper-evident packaging within a security briefcase, pouch or satchel.
Transfer	When transferring TOP SECRET information inside agency facilities: a) in Zones 3-5, transfer by hand or agency safe hand, and apply all necessary handling requirements. Can be uncovered if transfer is in close proximity and there is a low risk of unauthorised viewing b) in Zones 1-2, transfer by hand or agency safe hand, apply all necessary handling requirements and obtain written manager approval. When transferring TOP SECRET information outside agency facilities to another facility: a) written managerial approval must be obtained b) requirements for carrying outside agency facilities must be applied, including tamper-evident packaging c) transfer by hand, agency safe hand, safe-hand courier rated to BIL 5, or Department of Foreign Affairs and Trade (DFAT) courier. A receipt of transfer must be obtained.
Transmit	Electronic transmission of unencrypted TOP SECRET information must be over TOP SECRET secure networks. ASD's High Assurance Cryptographic Equipment must be used to encrypt TOP SECRET information for any communication that is not over a TOP SECRET network.
Official travel	TOP SECRET information and mobile devices that process, store or communicate TOP SECRET information, must not be stored or used outside appropriate agency facilities. Travelling in Australia with TOP SECRET information or mobile devices is not recommended, but if necessary: a) obtain written manager approval b) requirements for carrying outside agency facilities must be applied, including tamper-evident packaging

	c) information and/or device must be retained as carry-on baggage, and travel must not occur if airline requires baggage to be checked. TOP SECRET information must not be left unattended. Do not store while travelling (e.g. hotel room safes). If storage is required, it must be within an appropriate Australian agency facility. Do not travel overseas with TOP SECRET information or mobile devices that process, store or communicate TOP SECRET information. Seek DFAT advice on options to access information or devices at overseas destination. If access to TOP SECRET information or mobile devices provided at overseas destination: a) requirements for carrying outside agency facilities must be applied b) information and devices must be retained in personal custody (positive control) at all times or stored in an Australian agency's facilities.
Disposal	TOP SECRET information must be destroyed using a SCEC approved Class A shredder and destruction must be supervised.

Version control and change log

First publication	April 2023	
Revision	February 2024	
Next review date	December 2024	
Change Log	Policy issued	V1.0 April 2023
	Definition: 'core requirement' updated	V2.0 February 2024
	Definition: 'originator' updated	
	Definition: 'protected information' removed and replaced with 'security classified'	
	Definition: 'Responsible Executive' added	
	Definition: 'supplementary requirement' updated	
	Original supplementary requirement 'k' removed - (duplication of requirements)	
	BILs (p.38): removed financial specifics under OFFICIAL: Sensitive and PROTECTED column to suit Tasmanian context.	
	BILs (p.40): added Australian Government before 'Cabinet' under the PROTECTED column to suit national context.	

	BILs (p.41): removed financial value under Economy, at SECRET level for more relevant Tasmanian context.	

References and resources

Australian Government, sensitive and classified information, at www.protectivesecurity.gov.au/system/files/2023-11/policy-8-classification-system-pspf_0.pdf	
Australian Government, Information Security Manual, at www.cyber.gov.au/acsc/view-all-content/ism	
ASIO T4 Protective Security, Security Managers Handbook – Introduction to protective security measures available to authorised people via the GovTEAMS protective security community.	
New Zealand Government, information security, at www.protectivesecurity.govt.nz/information-security/	
SA Government, protecting information, at www.security.sa.gov.au/documents/SAPSF-INFOSEC1-Protecting-official-information-B425884-1.pdf	
Tasmanian Government, Information and Records Management Standard, at https://osa.tas.gov.au/wp-content/uploads/2023/08/Information-and-Records-Management-Standard.pdf	
Tasmanian Legislation	*Archives Act 1983*
	Personal Information Protection Act 2004
	Right to Information Act 2009
Tasmanian Government, Retention and Disposal Schedules, at https://osa.tas.gov.au/retention-and-disposal	

Tasmanian Government

Department of Premier and Cabinet
Resilience and Recovery Tasmania

Phone:
(03) 6232 7770

Email:
taspspf@dpac.tas.gov.au