South Australian Protective Security Framework

INFOSEC 1

PROTECTING OFFICAL INFORMATION

SOUTH AUSTRALIA

Government of South Australia

CONTENTS

POLICY

PURPOSE

1. This policy ensures all South Australian Government agencies protect their information assets from compromise. It outlines the South Australian Information Classification System (ICS) and associated guidance, which all agencies **must** use to protect the confidentiality, integrity and availability of all official information. The requirements of this policy are designed to mitigate against both intentional and accidental threats and reduce the impact on government business.

CORE REQUIREMENT

Protect official information against compromise[1]

SUPPORTING REQUIREMENTS

2. To protect official information against compromise, agencies[2] **must:**

   I. determine the appropriate classification and any protections that apply to official information

   II. set the classification at the lowest reasonable level to protect against compromise to the confidentiality, integrity or availability of all official information

   III. ensure all sensitive and security classified information (including emails) are marked with the correct protective markings

   IV. apply the Minimum Recordkeeping Metadata Requirements Standard to ensure metadata reflects any protective markings

   V. ensure all information is handled according to the classification and protective markings assigned to that information

   VI. seek permission from the information originator to make changes to the classification or protective markings

   VII. ensure processes for transferring or transmitting sensitive and security classified information deter and detect compromise

   VIII. ensure sensitive and security classified information is stored securely in an appropriate security container for the approved security zone

   IX. ensure sensitive and security classified information is disposed of securely

   X. be responsible for caveated and accountable material.

[1] Information compromise includes, but is not limited to loss, misuse, interference, unauthorised access, unauthorised modification, and unauthorised disclosure

[2] This policy applies to all South Australian public sector agencies (as defined in section 3(1) of the *Public Sector Act 2009*) and to any other person or organisation that is generally subject to the direction of a Minister of the Crown; all of which are referred to in this policy as “Agencies”.

GUIDANCE

CLASSIFYING OFFICIAL INFORMATION

3. Official information is all information created, sent and received as part of work of the South Australian Government. This information is an official record, and it provides evidence of what an agency has done and why. All official information **must** be protected according to the *business impact* that compromise of the information could cause from intentional or accidental threats.

4. Determining the appropriate classification of information in the South Australian Government promotes responsible management of information, open and transparent government and accountability for policies and practices that inappropriately or incorrectly classify information.

DETERMINING THE CLASSIFICATION

5. Classification enables agencies to protect their information in a consistent, organised and appropriate way. Table 1 lists the classifications that have been approved for use in the South Australian Government.

UNOFFICIAL	**UNOFFICIAL** can be used for non-work-related information. Use of the protective marking is optional, but may be required by ICT systems (e.g., emails).
OFFICIAL	**OFFICIAL** describes routine information created or processed by the South Australian Public sector with a low business impact. Use of the protective markings is optional, but recommended, and may be required by ICT systems (e.g., emails).
OFFICIAL: Sensitive [3]	**OFFICIAL: Sensitive** identifies sensitive but not security classified information. It is a single dissemination limiting marker (DLM) which indicates that compromise of the information may result in limited damage to an individual, organisation or government generally. Use of the protective marking is mandatory.

3 Examples of **OFFICIAL: Sensitive** information **may** include:

- official information governed by legislation that restricts or prohibits its disclosure, imposes certain use and handling requirements, or restricts dissemination (such as information subject to legal professional privilege, patient/practitioner confidentiality or some types of 'personal information', as covered in Premier's Circular PC012 Information Privacy Principles (IPPS) Instructions that may cause limited harm to an individual if disclosed or compromised). Where compromise of personal information, including sensitive information would lead to damage, serious damage or exceptionally grave damage, this information warrants a security classification. Although some personal information would not be considered sensitive for the purposes of this policy, the assessment of the damage to the individual caused by compromise **may** warrant the higher classification.
- commercial or economic data that, if compromised, would undermine a South Australian organisation or company, and/or provide an unfair economic advantage.
- information that, if compromised, would impede development of government policies.

PROTECTED [4]	**PROTECTED** is a security classification which indicates that compromise of the information may result in damage to the state or national interests, organisation or government generally. Use of the protective marking is mandatory.
SECRET[5]	**SECRET** is a security classification which indicates compromise of the information may result in serious damage to the state or national interests, organisations, or individuals. Use of the protective marking is mandatory.
TOP SECRET[6]	**TOP SECRET** is a security classification which indicates compromise of the information may result in exceptionally grave damage to the state or national interests, organisations, or individuals. Use of the protective marking is mandatory.

6. The information's originator is responsible for assigning the classification level, all protective markings and any additional handling instructions. The more valuable, important or sensitive the information is assessed to be, the greater the consequences could be. The potential consequences to individuals, organisation or the government caused by compromise of the information's confidentiality determines its classification.

7. Sometimes, not all the information in a document has the same classification. In these instances, the document **must** be classified according to the most sensitive or security classified information (see paragraph 28. *Paragraph grading indicators* for more information).

8. **Annex C: Table 1** provides examples of the potential business impacts from compromise to the confidentiality of official information. The BIL tool **should** be used to help achieve consistent classification of information across the South Australian Government.[7] The BIL tool is consistent with the Commonwealth PSPF.

9. The BIL tool can also be used for secondary assessments of the potential consequences from compromise of the availability or integrity of the information. If compromise to the integrity or availability is assessed to have a higher impact than compromise of the confidentiality, additional security measures (such as ICT, personnel or physical controls) **may** be warranted.

AVOIDING OVER-CLASSIFICATION

10. 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-

[4] Information classified at this level is considered security classified and must be handled in accordance with the requirements set out in this policy, including the for the user to be appropriately security cleared and need to know that information.

[5] Information classified at this level is considered security classified and must be handled in accordance with the requirements set out in this policy, including the for the user to be appropriately security cleared and need to know that information.

[6] Information classified at this level is considered security classified and must be handled in accordance with the requirements set out in this policy, including the for the user to be appropriately security cleared and need to know that information.

[7] The BILs are not intended to be proscriptive, but rather can be used to help determine the appropriate classification

to-know. This requirement also helps to reduce over-classification of official information.

11. Over-classification can result in access to official information being unnecessarily limited or delayed, onerous administration and procedural overheads which add to costs and classifications being devalued or ignored by staff and recipients.

12. The originator **must not** apply sensitivity or security classified markings to information where it:

    I. restrains competition

    II. hides violations of law, inefficiency, or administrative error to prevent embarrassment to an individual or agency

    III. prevents or delays the release of information that does not need protection in the state or national interest.

CAVEATS AND ACCOUNTABLE MATERIAL

13. A caveat is a warning that the information contained has special protections *in addition to* those indicated by the classification.[8] There are four broad types of caveat:

    I. sensitive compartment information (codeword)[9]

    II. foreign government markings

    III. special handling instructions

    IV. releasability caveats

14. Accountable material is information requiring strict control over its access and movement. Accountable material includes:

    I. **TOP SECRET** security classified information

    II. some types of caveated information, being:

        a. all codeword information

        b. select special handling instruction caveats, particularly **SA CABINET** material at any classification

        c. any classified information designated as accountable material by the originator[10]

15. All agencies **must** be responsible for caveated or accountable material in accordance with the originator's special handling requirements.

---

[8] Caveats are not a classification and must only appear with an appropriate classification marking

[9] A codeword indicates the information is of sufficient sensitivity that it requires protection in addition to that offered by a security classification. Access is controlled by strict need-to know requirements. Use of codewords is primarily within the national security community and the meaning is unrelated to the subject of the information. If an agency receives codeword information in any form, agencies must seek specific guidance from the originating entity.

[10] Accountable material **may** vary from agency to agency and could include material such as budget papers, tender documents and sensitive ministerial briefing documents.

USING CAVEATS

16. The special handling requirements of a caveat apply *in addition to* the classification's handling requirements. Caveats **must not** be removed or changed without approval of the information's originator.

17. **Table 1** outlines the types of caveats that **may** be encountered, or required, in the South Australian Government.[11] See paragraph 20. *Protections for official information* for guidance on how to apply caveats correctly.

[11] Additional guidance on the use of caveats, including the types that may be encountered on Australian Government material, is available in the Sensitive Material Security Management Protocol and the Security Caveat Guidelines, which can be accessed via GovTeams.

Table 1 - Types of caveats

Caveat type	Caveat	What special handling requirements does this caveat impose?	What special handling requirements does this caveat impose?
Special handling instructions Special handling instructions indicate particular precautions for information handling.	**SA CABINET**	The **SA CABINET** caveat identifies any material that: a. is prepared for the purpose of informing the South Australian Cabinet b. reveals the decisions and/or deliberations of the South Australian Cabinet c. is prepared by departments to brief their ministers on matters proposed for South Australian Cabinet consideration d. has been created for the purpose of informing a proposal to be considered by the South Australian Cabinet.	The South Australian Cabinet Handbook specifies handling requirements for South Australian Cabinet documents. This includes applying a classification of at least **OFFICIAL: Sensitive** to all South Australian Cabinet documents and associated records
	EXCLUSIVE FOR (named person)	The EXCLUSIVE FOR caveat identifies material intended for access by a named recipient only.	Access to **EXCLUSIVE FOR** material is limited to a named person, position title or designation. A classification of at least **OFFICIAL: Sensitive** must be applied.
	NATIONAL CABINET	The **NATIONAL CABINET** caveat identifies any material that: a. is prepared for the purpose of informing the National Cabinet b. reveals the decisions and/or deliberations of the National Cabinet c. is prepared by departments to brief their ministers on matters proposed for the National Cabinet consideration	The Commonwealth's Cabinet Handbook specifies handling requirements for Cabinet documents. Information marked with the **NATIONAL CABINET** caveat is to be handled in accordance with Cabinet conventions and within legal frameworks and processes

		d. has been created for the purpose of informing a proposal to be considered by the National Cabinet.	such as Freedom of Information, parliamentary inquiries, and judicial processes. This caveat can be applied to information marked as **OFFICIAL: Sensitive** or with a security classification. Access to information marked **NATIONAL CABINET** must be consistent with the handling requirements of the classification and any additional protective markings.

Caveat types	Caveat	What kinds of information does this type of caveat cover?	What special handling requirements does this caveat impose?
Releasability caveats **Releasability caveats limit access to information based on citizenship.** **Agencies may need to be aware of releasability caveats which are primarily used within the national security community.**	**Releasability caveats appear only with security classifications (PROTECTED or higher)** **There are three (3) releasability caveats used across government:**		
	Australian Eyes Only (**AUSTEO**)	The **AUSTEO** caveat indicates only Australian citizens can assess the information. Additional citizenships do not preclude access.	Information marked **AUSTEO** is only passed to, or accessed by, Australian citizens. While a person who has dual Australian citizenship **may** be given **AUSTEO**-marked information, in no circumstance **may** the Australian citizenship requirement be waived.

	Australian Government Access Only (**AGAO**)	In limited circumstances, **AGAO** is used by National Intelligence Community (NIC) agencies	Non-NIC agencies must handle **AGAO** material as if it were marked **AUSTEO**.
	Releasable To (**REL**)	The Releasable To (**REL**) caveat identifies information that has been released or is releasable to the indicated foreign countries only[12]	For example, REL AUS/CAN/GBR/NZL/USA means that the information may be passed to citizens of Australia, Canada, United Kingdom, New Zealand and the United States of America only. The caveat is an exclusive marking that disqualifies a third-party national seconded or embedded in a foreign government entity from accessing the information.
Foreign government markings		**Foreign government markings** are applied to material created by Australian agencies from foreign source information.	If an agency receives foreign government marked information, agencies must apply the South Australian Protective Security Framework (SAPSF) policy Security governance for international sharing. Agencies must safeguard foreign government marked information to at least the equivalent to that required by the foreign government providing the information.

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

INFORMATION MANAGEMENT MARKERS

18. Information Management Markers (IMM)[13] are optional markings agencies **may** choose to use to help manage the security of and access to information classified **OFFICIAL: Sensitive** of higher. The IMMs can be used to help agencies and users to identify the type of information contained. See paragraph 20. *Applying protective markings* for guidance on how to apply IMMs correctly.

19. The four IMMs designated for use in South Australia are:

Legal privilege	Restrictions on access to, disclosure or use of, information covered by legal professional privilege
Legislative secrecy	Restrictions on access to, disclosure or use of, information covered by legislative secrecy provisions
Personal privacy	Restrictions, under the *Premier's Circular PC012 Information Privacy Principles (IPPS) Instructions*, on access to, disclosure or use of, personal information collected or received
Medical in confidence	Restrictions on access to, disclosure or use of, information covered by practitioner/patient confidentiality or legislative requirements

PROTECTIONS FOR OFFICIAL INFORMATION

APPLYING PROTECTIVE MARKINGS

20. Agencies **must** use protective markings to indicate to users and systems the information's classification and any additional handling requirements. Protective markings help users (as a visual mark) and systems (e.g., agency's email gateway) control the distribution of information.

21. The originator **must** clearly identify sensitive and security classified information by using the appropriate protective markings.

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

    I. classification

    II. foreign government information markings (if any)

    III. caveats or other special handling instructions (if any)

    IV. information management markers (optional, if any)

23. **UNOFFICIAL** is an optional marking that **may** be used to identify information generated for personal or non-work-related purposes (marking **may** be required on some ICT system e.g., email).

24. **OFFICIAL** describes routine information produced or processed by the public sector. Use of the **OFFICIAL** marker is optional and **may** be used to identify official information that is not sensitive, or security classified purposes (marking **may** be required on some ICT system e.g., email). **OFFICIAL** indicates the information requires no specific protections and no consequences are caused by its public release.

[13] IMMs are not classification and **must** only appear with an appropriate classification marking

AGENCY SPECIFIC AND OTHER PROTECTIVE MARKINGS

25. Agency specific and other protective markings are not recognised by this policy. A standard set of markings ensures common understanding, consistency and interoperability across systems and government entities. Creation of markings outside this policy may confuse users about appropriate handling protections and increase the likelihood of compromise.

TEXT-BASED PROTECTIVE MARKING

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

27. Text-based protective markings **should** be**:**

    I. in capitals (other than for DLMs and IMMs), in a large, plain text font, in a distinctive colour (red preferred)

    II. centred and placed at the top and bottom of each page

    III. separated by a double forward slash(***//***) to help to clearly differentiate each marking.

For example:

OFFICIAL: Sensitive//Legal privilege

PROTECTED//SA CABINET

PARAGRAPH GRADING INDICATORS

28. Paragraph grading indicators are useful where there is a need to identify the classification of individual paragraphs or sections, in addition to the documents overall classification and protective marking (the paragraph or section with the highest classification within the document dictates the document's overall classification and protective markings). Paragraph grading indicators are **optional.**

29. It is **recommended** that paragraph grading indicators appear:

    I. in the same colour as the text of the document

    II. in brackets () at the start or end of each paragraph or in the margin adjacent to the first letter of the paragraph

    III. written in full, or abbreviated by the first letter(s) of the markings, as follows:

        a. (UO) for **UNOFFICIAL**

        b. (O) for **OFFICIAL**

        c. (O:S) for **OFFICIAL: Sensitive**

        d. (P) for **PROTECTED**

        e. (S) for **SECRET**

        f. (TS) for **TOP SECRET**

COLOUR-BASED PROTECTIVE MARKING

30. For security classified information, if text-based protective markings cannot be used (e.g., certain media or assets e.g., USB key), the following colour-based protective markings **must** be used:[14]

PROTECTED	SECRET	TOP SECRET
BLUE	SALMON (PINK)	RED
R 79, G 129, B 189	R 229, G 184, B 183	R 255, G 0, B 0

31. There are no requirements to use RGB colour markings for OFFICIAL: Sensitive information, although, if required, a yellow colour **should** be used.

32. **Annex C: Table 2** aligns each classification to its BIL, definition, protective marking, handling, and access instructions.

PROTECTIVE MARKING IN METADATA

33. 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.

34. For consistency, State Records produced the Minimum Recordkeeping Metadata Requirements Standard in 2020 which provides standardised metadata terms and definitions for consistency across government. The Standard identifies the metadata properties essential for agency management and use of business information, including the appropriate application of South Australia's Information Classification System (ICS) as outlined in the SAPSF.

35. All agencies **must** apply the Standard to ensure agency records are managed according to best record management practices, as per the State Records Act 1997.

36. The metadata of information on ICT systems **must** identify:

    I. the classification of the information

    II. the properties of any caveat used

    III. the 'rights' property (IMMs)[15]

PROTECTIVE MARKING IN EMAIL

37. The preferred approach for marking email is to apply the protective markings to the internet message header extension, consistent with the Email protective marking standard, which provides guidance for applying protective markings (and, where relevant, information management markers) on emails exchanged within, between and outside of South Australian Government agencies.

38. All agencies **must** ensure that where emails are printed, classification protective markings are still visible.

[14] The colour-based markings use the RGB (Red, Green, Blue) model. The RGB values listed for security classified information **should** be used, unless the exact values cannot be applied.

[15] While the use of IMMs is optional, the metadata **must** identify when a rights property has been used, such as an IMM.

LIMITING ACCESS TO SENSITIVE AND SECURITY CLASSIFIED INFORMATION

39. Most official information **can** be shared, where required. Agencies **mus**t make official information available to those with a need-to-know (NTK). Applying the NTK principle reduces the risk of unauthorised access or misuse of information.

40. For information identified as security classified, an appropriate security clearance[16] **must** be obtained in addition to NTK.

RECORD OF DISSEMINATION - AUDIT, LOGS AND CLASSIFIED DOCUMENT REGISTERS

41. Highly classified information (**TOP SECRET** information or accountable material) **must** be monitored via an auditable register (e.g., Classified Document Register) to keep track of incoming and outgoing material, access, transfers or copying of that material.

USING OFFICIAL INFORMATION

42. Access to, and use of, official information **must** maintain the protections required by the classification assigned to it. This requirement extends to the physical environment the information is being used in, in addition to any handling instructions mandated by the classification.

43. When sensitive and security classified information is being used (e.g., able to be read, viewed, heard or comprehended) it may be at a higher risk of compromise, depending on the physical environment it is being used in. Agencies **must** minimise the risks of compromise by combining the required protections and controls of this policy, with the required physical security measures of SAPSF policy Physical security.

44. In conjunction with those controls and measures, it is imperative that employees demonstrate good security practices and awareness when using sensitive and security classified information, including:

    I. remaining vigilant and aware of their environment, including awareness of who might have access to that environment and to information they are not authorised to access.

    II. selecting work environments based on their suitability to use the required information

    III. taking all necessary or available steps to reduce the risk of unauthorised access, use or removal of information

    IV. correct physical handling procedures when information is being carried or not in active use.

WORKING AWAY FROM THE OFFICE

45. Any work undertaken away from an agency's facilities is considered 'away from the office', which includes mobile computing, communications and teleworkers. Physical security requires that all agencies **must** consider what security measures are required to enable employees to work securely away from the office. This includes the use and/or storage of sensitive or security classified information.

[16] For guidance on obtaining a personnel security clearance, see in the SAPSF policies Recruiting employees and Accessing official information

46. Working away from the office includes:
    I. another agency or entity's facilities
    II. private homes (e.g., for regular ongoing or occasional home-based work)
    III. public spaces
    IV. facilities overseas
47. This requirement **must** also extend to ensuring employees are able to securely transport sensitive and security classified information between locations or to another individual (see Transmitting or transferring sensitive and security classified information, or physically removing it from agency facility) and store appropriately when not in use (see Storing sensitive and security classified information).
48. The employee that removes the sensitive or security classified information from an agency's facilities is then **responsible for** handling the information in accordance with the protections required by the classification and location.
49. See **Annex C: Table 3** for the minimum protections for information transmission and transfer when working away from the office.

MOBILE COMPUTING AND COMMUNICATION

50. Mobile devices such as laptops, tablets and smart phones all enable work to be undertaken away from entity facilities due to their portable nature. While these devices can be significant business enablers, there is a significant risk associated with their use that **must** be addressed. Employees **must** consider and demonstrate the same level of good security practice and awareness when using mobile devices to access and undertake official business.
51. Agencies **must** ensure that the use of privately-owned devices does not present an unacceptable security risk, and it is **recommended** that their use be avoided, where possible. Further guidance on mobile device security is available in the South Australian Cyber Security Framework (SACSF).

USING OFFICIAL INFORMATION DURING OFFICIAL TRAVEL OUTSIDE AUSTRALIA

52. Travel outside Australia for official purposes presents additional risks to employees, official information and assets. Agencies are **responsible for** implementing policies and procedures that mitigate any risk posed by travel outside Australia to employees and any sensitive or security classified information they may be travelling with, including mobile devices or media containing such information.
53. It is **recommended** that agencies consider providing location-specific advice and consult with relevant authorities prior to travelling, such as the Office of the Chief Information Officer (OCIO), South Australia Police, the Department of Foreign Affairs and Trade or the Australian Security Intelligence Organisation, especially where identified risks cannot be appropriately mitigated
54. Personnel undertaking overseas travel for official purposes **must** complete a Post-Travel Security Report and submit to SAPSF@SA.GOV.AU within 7 days of returning.

SANITISING, DECLASSIFYING OR RECLASSIFYING INFORMATION

55. Information may sometimes require modification (sanitising) to allow it to be shared more widely. The classification of information **may** be changed by the originator by editing, disguising or altering information to allow greater sharing. Elements that need to be protected when sanitising information include intelligence, sources, methods,

capabilities, analytical procedures or privileged information. Once the content has been sanitised, the information can be declassified or reclassified.

56. The originator of the information remains responsible for sanitising, reclassifying or declassifying.

DETERMINING WHEN TO DECLASSIFY

57. Information declassification **may** take place when the information is no longer expected to cause the consequences as originally assessed in the classification.
58. Under the *State Records Act 1997*, the originator is responsible for determining when records in the custody of the archive become publicly accessible. The originator **should** consider the period of time the information might be expected to have consequences and assign an appropriate timeframe to avoid information remaining restricted or classified.
59. State Records of South Australia provides guidance to determining the appropriate timeframe under the *Public Access Determinations.*

TRANSMITTING OR TRANSFERRING SENSITIVE AND SECURITY CLASSIFIED INFORMATION, OR PHYSICALLY REMOVING IT FROM AGENCY FACILITIES

60. The risk of compromise increases when sensitive and security classified information is in transit (e.g., sent across the internet or between physical locations) and when an agency does not have control over the entire transmission network. As such, agencies **must** only transmit or transfer information for official purposes and **must** use transmission means which deter and detect compromise.
61. NTK **must** be applied when transmitting or transferring sensitive and security classified information. Recipients **must** also hold the appropriate security clearance, where required.
62. Agencies **should** identify recipients of sensitive and security classified information by:
    I. the specific position, appointment or named individual [17]
    II. a full location address (e.g., not a post office box for physical delivery as this may be unattended)
    III. an alternative individual or appointment where relevant (e.g., TOP SECRET or accountable material)
63. 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. This can be achieved by:
    I. using appropriate encryption methods[18] for transferring information over a public network or though unsecured spaces
    II. double envelopes for physical information by placing security classified or accountable material inside two sealed envelopes:
        a. the inner envelope **must** give evidence of tampering, e.g., by sealing with a Security Construction and Equipment Committee (SCEC)-

[17] The EXCLUSIVE FOR caveat may be used if the information is classified OFFICIAL: Sensitive or above

[18] For information on cryptography, see the SACSF

approved tamper evident seal.[17] The classification **should** be marked conspicuously on the inner envelope.

b. The outer envelope protects the inner envelope. This envelope **should not** be marked with the classification or other protective markings.

III. single use envelopes approved by SCEC for:

a. an inner envelope

b. single opaque envelopes in place of envelope

c. an outer envelope used to enclose a number of inner envelopes where initial delivery will be to a registry or similar

II. a single paper envelope in conjunction with a security briefcase[19] or approved multi-use satchels, pouches or transit bags[20]

TRANSFERRING INFORMATION VIA DEVICES

64. Devices such as laptops, mobile phones and USBs can be used to transfer and transmit information. The requirement to deter and detect information compromise applies to sensitive and security classified information transferred on such devices. Multi-factored authentication, password protection and remote wiping capabilities **should** be considered. For more guidance refer to the SACSF.

65. Methods to control the transmission and transfer of information include:

I. use of receipts:

a. Receipts **should** identify the date and time of dispatch, the sender's name and a unique identifying number. Receipts **should** be used for transmission or transfer of all classified information.

b. If using receipts, agencies **should** have a receipt system to record every handover of information (e.g., two-part receipt placed in the inner envelope with the information, allowing the addressee to keep one part and return the other to the sender).

II. safe hand:

a. safe hand means information is given to the addressee in the care of an authorised person or succession of authorised people who are responsible for the safe carriage of the information.

b. sending information via safe hand establishes an audit trail that provides confirmation that the addressee received the information and helps to ensure the item is transferred to its intended destination. Each handover **should** include a receipt showing the unique identifying number, time and date of the handover, and the name and signature of the recipient.

c. to send information via safe hand, agencies **must:**

[19] see the SCEC-approved security equipment evaluated product list

[20] refer to the SCEC-Security Equipment Guide of Briefcases for the carriage of security classified information

- assign a unique identification number (generally a receipt number)
- transfer in a security briefcase[21] or approved mailbag[22]
- ensure information is not left unattended (except when in the cargo compartment of an aircraft)

III. carriage by a SCEC-endorsed commercial courier:

a. a number of commercial courier services have been endorsed by SCEC. Contact ASIO-T4 by email t4ps@t4.gov.au or see the ASIO-T4 *Protective security circular (PSC) 172* for advice on SCEC endorsed commercial couriers.

b. Commercial couriers can be useful in transferring valuable material such a pharmaceuticals and money (note SCEC-endorsed couriers are not assessed for the transfer of these items. Special arrangements, such as armed escorts, **may** be necessary in certain circumstances.

c. Special handling requirements **may** apply to caveated information. This **may** preclude the use of a commercial courier when using certain caveats.

66. Transmission or transfer of official, but not sensitive or security classified information is on a common-sense basis. While not required by this policy, agencies **should** transfer or transmit information by means which deter and detect compromise.
67. **Annex C: Table 3** provides information on the minimum protections for information transmission and transfer.

STORING SENSITIVE AND SECURITY CLASSIFIED INFORMATION

68. The Australian Government Information Management Standard requires that agencies ensure their information assets are accessible for as long as needed and are shared appropriately (subject to access, security and privacy rules) within a protected and trusted environment.
69. It is expected that all agencies implement information classification practices and protective marking procedures that recognise and indicate the protections information requires, and that those protections are removed as soon as they no longer apply, when the sensitivity or need for security classification diminishes.
70. All agencies **must** store information securely and preserve it in a usable condition for as long as required for business needs and community access. A secure and suitable storage environment is one that prevents unauthorised access, duplication, alteration, removal and destruction.
71. When sensitive and security classified information is unattended or not in use, it is considered stored, and **must** be secured in an appropriate security container for the approved security zone. This requirement extends to mobile devices holding sensitive or security classified information. It is **recommended** that encryption[16] is active when mobile devices are not in use.

[21] see the SCEC-approved security equipment evaluated product list
[22] see the SCEC-approved security equipment evaluated product list

72. **Annex C: Table 4** provides guidance on the minimum use and storage requirements for sensitive and security classified information, while further guidance on physical security zones can be found in SAPSF policy Physical security.

CLEAR DESK, END SESSION AND SCREEN LOCKING PROCEDURES

73. It is **recommended** that all agencies implement clear desk, end session and screen locking procedures to mitigate the risk of compromise to unattended information or resources. Such procedures require employees to secure all hard-copy documents, ensure access to sensitive and security classified information is disabled (e.g., closing/locking security containers, logging out of secure system access correctly) and lock device screens when not being used.

DISPOSING OF OFFICIAL INFORMATION

74. Once official information no longer has a business need or value, it may not need to be kept by the agency. Any sensitive or security classified information that is no longer required by an agency **must** be disposed of in a secure manner. Failure to adequately dispose of sensitive of security classified information can result in serious compromise, with serious consequences, including loss of confidence in the South Australian Government.

75. Under the *State Records Act 1997*, **dispose of** means:

    I. destroy or abandon the record

    II. carry out an act the result of which means it is no longer possible to reproduce the whole or part of that information

    III. transfer or deliver ownership or possession of or sell the information

76. Disposal includes the physical destruction of paper records; destruction of electronic records including deleting emails, documents or other data from business systems and the transfer of records to a non-South Australian Government entity.

77. Under Section 23 of the *State Records Act 1997*, information disposal can only take place:

    I. Through a determination made by the Director [Manager] State Records, and

    II. With the approval of the State Records Council.

78. In South Australia, a determination for the purposes of *Section 23* of the *State Records Act* is in the form of a disposal schedule. For guidance, see *State Records of South Australia.*

DESTROYING SENSITIVE AND SECURITY CLASSIFIED INFORMATION IN PHYSICAL FORM

79. Physical information **may** be destroyed in a number of ways. Commonly used destruction methods include:

    I. pulping

    II. burning

    III. pulverising using hammermills

    IV. disintegrating or cutting and reducing the waste particle size

V. shredding using crosscut shredders (strip shredders are **not** approved for destruction of security classified information

80. Methods for destruction of digital information include:

I. digital file shredding

II. degaussing by demagnetising magnetic media to erase recorded data

III. physical destruction of storage media through pulverisation, incineration or shredding (the SACSF provides guidance on sanitisation and destruction of ICT equipment and storage media)

IV. reformatting, if it can be guaranteed that the process cannot be reversed.

ENGAGING COMMERCIAL DESTRUCTION SERVICES

81. Commercial providers **may** be used to destroy classified information. Agencies **must** review the appropriateness of a commercial provider's collection process, transport, facility, procedures and approved equipment when considering engaging their destruction services. ASIO-T4 provides advice on engaging destruction services though Protective security circular 167 – Destruction of sensitive and security-classified information – (PSC 167), available through GovTeams.

82. Criteria for commercial destruction includes:

I. Ensuring classified information is attended at all times and the vehicle and storage areas are appropriately secured

II. Ensuring that destruction is performed immediately after the material has arrived at the premises

III. Ensuring that destruction is witnessed by an entity representative

IV. Ensuring destruction service staff have a security clearance to the highest level of security classified information being transported and destroyed, or appropriately security cleared entity staff escort and witness the destruction.

83. There are a number of commercial destruction services that hold National Association for Information Destruction AAA certification (with endorsement in PSC 167 External destruction of security classified information). These commercial providers are able to destroy security classified information.

84. It is **recommended** information classified **TOP SECRET**, or accountable material, be destroyed within entity premises. The originator **should** request notification of destruction. The originator of accountable material **may** apply special handling conditions that prevent information destruction being contracted out.

85. **Annex C: Table 5** summarises the minimum handling protections for disposal of physical sensitive and security classified information, ICT media and equipment.

SECURITY INCIDENTS INVOLVING SECURITY CLASSIFIED INFORMATION

86. Suspected or actual compromise of security classified information is considered a security incident, and SAPSF policy Security governance requires that agencies notify affected agencies of security incidents.

87. Agencies **must** notify the owner or originator of security classified information as soon as practicable following suspected or actual compromise. It is

also **recommended** that loss or compromise of **SECRET** or **TOP SECRET** information is reported to the Department of the Premier and Cabinet and to the Australian Security Intelligence Organisation.

RELATED DOCUMENTS

88. Legislation, policies and documents referenced in this policy that may be relevant to the handling of official information include:

- *State Records Act 1997* (SA)
- *Premier's Circular PC012 Information Privacy Principles (IPPS) Instructions*
- *Public Access Determinations*
- *South Australian Cyber Security Framework*
- *Health Care Act 2008*, *Mental Health Act 2009*, *Children and Young People (Safety) Act 2017*
- *Protective Security Policy Framework*
- *Information Security Manual*

DOCUMENT CONTROL

Approved by: Chief Executive, Department of the Premier and Cabinet	Date of first approval: 20 April 2020
Revision number: 2.0	Date of review: 26 October 2022
Next review date: December 2024	Contact: sapsf@sa.gov.au

CHANGE LOG

Version	Date	Changes
1.0	25/11/2019	First issue of policy
1.1	20/04/2020	Policy title changed to 'Protecting official information' Classification protective marking examples changed to red colour Removal of word 'your' throughout entire document
1.2	21/08/2020	Definition of 'personnel' updated Definition of 'employee' and 'visitor' added. Supporting requirement IV moved from SAPSF policy INFOSEC2: Accessing official information Guidance for NATIONAL CABINET caveat added to Table 1 – Types of caveats Guidance for marking UNOFFICIAL and OFFICIAL information clarified (paras 23 & 24) Paragraph grading indicators section added (paras. 28 & 29) RGB colour codes added to Colour-based protective marking. Guidance for colour marking OFFICIAL: Sensitive added (para 31). Colour markings in document tables updated. Guidance for Protective marking in metadata and email amended (paras 33-38) Section Using official information added (paras 42-52) Guidance for Storage of security classified information amended (para 69) Section Clear desk, end session and screen locking procedures added (para 71) Section Security incidents involving security classified information (paras 84-85)
1.3	09/11/2020	Requirements for home-based work in Annex Table 3 amended.

2.0	30/11/2022	Supporting requirement IV updated to include the *Minimum Record keeping Metadata Requirements Standard* Guidance for Working Away from the Office updated (para 46-50)
2.1	19/09/2023	Added requirement to complete Post-Overseas Travel Security Report

ANNEX A: MAPPING PREVIOUS AND NEW CLASSIFICATIONS AND SENSITIVITY MARKINGS IN SOUTH AUSTRALIA

Mapping Classifications

This table maps the new classifications and sensitivity markings of the ICS against the former classifications and protective markings used in South Australia

<table>
<tr><th>Then
(pre-1 December 2019)</th><th>To</th><th>Now (post-1 December 2019</th><th></th></tr>
<tr><td>TOP SECRET</td><td>no change</td><td>TOP SECRET</td><td rowspan="4">Security Classification</td></tr>
<tr><td>SECRET</td><td>no change</td><td>SECRET</td></tr>
<tr><td>CONFIDENTIAL</td><td>Discontinued</td><td>-</td></tr>
<tr><td>PROTECTED</td><td>no change</td><td>PROTECTED</td></tr>
<tr><td>Sensitive: SA Cabinet</td><td>DLM → Caveat</td><td>SA CABINET[23]</td><td rowspan="9">Non-security classifications[24]</td></tr>
<tr><td>Sensitive</td><td rowspan="6">DDLMs → DLM</td><td rowspan="5">OFFICIAL: Sensitive</td></tr>
<tr><td>Sensitive: Personal</td></tr>
<tr><td>Sensitive: Legal</td></tr>
<tr><td>Sensitive: Medical</td></tr>
<tr><td>Sensitive: Commercial</td></tr>
<tr><td>For Official Use Only[25]</td><td rowspan="2">OFFICIAL</td></tr>
<tr><td>PUBLIC</td><td>→</td></tr>
<tr><td>-</td><td>New classification</td><td>UNOFFICIAL</td></tr>
</table>

Information Management Markers (IMM) are optional protective markings which **may** be used where a legislative or professional restriction may apply to disclosure of information contained. IMMs **must** only be used in addition to a classification of OFFICIAL: Sensitive or higher.

[23] Caveat must only appear with classification of OFFICIAL: Sensitive or higher

[24] UNCLASSIFIED was previously used to describe information without a security classification. Under the ICS, unclassified has been replaced by 'non-security classification'.

[25] In South Australia, some information previous classified as FOR OFFICIAL USE ONLY may now be classified either OFFICIAL: Sensitive or OFFICIAL. Agencies must consider the potential business impact when making this determination.

INFORMATION MANAGEMENT MARKERS	**LEGISLATIVE SECRECY**
	PERSONAL PRIVACY
	LEGAL PRIVILEGE
	MEDICAL IN CONFIDENCE

ANNEX B: HISTORICAL CLASSIFICATIONS AND SENSITIVITY MARKINGS IN SOUTH AUSTRALIA

Historical classification or sensitivity marking	Key dates	Current sensitive or classified information level equivalency	Handling
CONFIDENTIAL[26]	Recognition of CONFIDENTIAL ceased in South Australia on 1 December 2019. The classification is grandfathered[27] for South Australian agencies until 1 December 2020.	None established. Consider the harm and apply corresponding security classification marking	Historical handling protections remain. See Annex A Table 2 of the PSPF policy Sensitive and Classified Information for CONFIDENTIAL classified information handling protections.
For Official Use Only (FOUO)*	FOUO replaced on 1 December 2019. Recognition of FOUO ceases on 1 December 2020.	FOUO is equivalent to the current **OFFICIAL: Sensitive** level, although some information previously classified FOUO may now be classified **OFFICIAL**. Agencies must consider the potential business impact when making this determination	Handling of FOUO information is as per SAPSF requirements for **OFFICIAL: Sensitive** information.
Sensitive	Sensitive replaced on 1 December 2019. Recognition of Sensitive ceases on 1 December 2020.	Unless otherwise classified, Sensitive is equivalent to the current **OFFICIAL: Sensitive** level. The (optional) Legislative secrecy information management marker may be applied.	Handling of Sensitive information is: a. if classified, as per the identified classification level b. if not classified, as per SAPSF requirements for **OFFICIAL: Sensitive** information.
Sensitive: SA Cabinet*	Sensitive: SA Cabinet replaced on 1 December 2019. Recognition of Sensitive: SA Cabinet ceases on 1 October 2020.	Sensitive: SA Cabinet is equivalent to the current **SA CABINET** caveat.	Handling of Sensitive: SA Cabinet information is as per: a. the identified classification level and b. SAPSF requirements for **SA CABINET** caveat c. South Australian Cabinet Handbook.
Sensitive: Legal*	Sensitive: Legal replaced on 1 December 2019. Recognition of Sensitive: Legal ceases on 1 December 2020.	Unless otherwise classified, Sensitive: Legal is equivalent to the current **OFFICIAL: Sensitive** level. The (optional) Legal privilege information management marker may be applied.	Handling of Sensitive: Legal information is: a. if classified, as per the identified classification level b. if not classified, as per SAPSF requirements for **OFFICIAL: Sensitive** information.
Sensitive: Personal*	Sensitive: Personal replaced on 1 December 2019. Recognition of Sensitive: Personal ceases on 1 December 2020.	Unless otherwise classified, Sensitive: Personal is equivalent to the current **OFFICIAL: Sensitive** level. The (optional) Personal privacy information management marker may be applied.	Handling of Sensitive: Personal information is: a. if classified, as per the identified classification level b. if not classified, as per SAPSF requirements for **OFFICIAL: Sensitive** information.
Sensitive: Medical	Sensitive: Medical replaced on 1 December 2019. Recognition of Sensitive: Medical ceases on 1 December 2020.	Unless otherwise classified, Sensitive: Medical is equivalent to the current **OFFICIAL: Sensitive** level. The (optional) Medical in confidence information management marker may be applied.	Handling of Sensitive: Medical information is: a. if classified, as per the identified classification level **b.** if not classified, as per SAPSF requirements for **OFFICIAL: Sensitive** information.

[26] *This classification or sensitivity marking was replaced in the Australian Government on 1 October 2018, with recognition ceasing on 1 October 2020

[27] 'Grandfathering' of information classified CONFIDENTIAL mean that agencies do not need to reclassify existing holdings and protection requirements will remain the same as before its cessation

Sensitive: Commercial	Sensitive: Commercial replaced on 1 December 2019. Recognition of Sensitive: Commercial ceases on 1 December 2020.	Unless otherwise classified, Sensitive: Confidential is equivalent to the current **OFFICIAL: Sensitive** level.	Handling of Sensitive: Commercial information is: a. if classified, as per the identified classification level **b.** if not classified, as per SAPSF requirements for **OFFICIAL: Sensitive** information.
PUBLIC	PUBLIC replaced on 1 December 2019. Recognition of PUBLIC ceases on 1 December 2020.	PUBLIC has been replaced by the classification **OFFICIAL.**	No special protections or handling requirements apply to **OFFICIAL** information.
HIGHLY PROTECTED	Recognition of HIGHLY PROTECTED ceased on 1 August 2012.	HIGHLY PROTECTED is equivalent to the current **SECRET** classification	Handling of HIGHLY PROTECTED information is as per SAPSF requirements for **SECRET** information.
RESTRICTED	Recognition of RESTRICTED ceased on 1 August 2012.	RESTRICTED is equivalent to the current **OFFICIAL: Sensitive** level.	Handling of RESTRICTED information is as per PSPF requirements for **OFFICIAL: Sensitive** information.
X-IN-CONFIDENCE	X-IN-CONFIDENCE classification ceased on 1 August 2012 and was replaced by the Dissemination Limiting Markers.	X-IN-CONFIDENCE is equivalent to the current **OFFICIAL: Sensitive** level.	Handling of X-IN-CONFIDENCE information is as per SAPSF requirements for **OFFICIAL: Sensitive** information.

ANNEX C

ANNEX C: TABLE 1 - BUSINESS IMPACT LEVEL TOOL

Note: The BIL Tool is not intended to be proscriptive, but a tool to assist agencies to assess confidentiality, integrity and availability in a consistent manner across the South Australian Government. Where an agency cannot, or chooses not to, apply a higher classification to sensitive security classified information, that agency must document acceptance of the higher level of risk, and acknowledge of the potential consequences were that aggregation to be compromised. The accountable authority must be responsible for this risk.

SENSITIVE INFORMATION			SECURITY CLASSIFIED INFORMATION		
Classification	**OFFICIAL**	**OFFICIAL: Sensitive**	**PROTECTED**	**SECRET**	**TOP SECRET**
Business Impact Levels	**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 the South Australian public sector	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.
Sub-impact category: Potential impacts to individuals from compromise of the information					
Dignity or safety of an individual (or those associated with the individual)	Information from routine business operations and services. This includes personal information as defined in Premier's Circular PC012 Information Privacy Principles (IPPS) Instructions.[28]	Limited damage to an individual is compromise of personal information[29] that would lead to: a. potential harm, for example injuries that are not serious or life threatening or b. b. discrimination, mistreatment, humiliation or undermining an individual's dignity or safety that is not life threatening.	Damage to an individual is: a. 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: a. 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 many people.
Sub-impact category: Potential impacts to organisations from compromise of the information					
Entity operations, capability, and service delivery	Information from routine business operations and services.	Limited damage to entity operations is: a. degradation in organisational capability to an extent and duration that, while the entity can perform its primary functions, the effectiveness of the functions is noticeably reduced b. minor loss of confidence in government.	Damage to entity operations is: a. a degradation in, or loss of, organisational capability to an extent and duration that the entity cannot perform one or more of its primary functions a. b. major loss of confidence in government.	Serious damage to entity operations is: a. a severe degradation in, or loss of, organisational capability to an extent and duration that the entity cannot perform any of its functions b. directly threatening the internal stability of South Australia.	Not applicable[30]
Entity assets and finances, e.g. operating budget	Information compromise would result in insignificant impact to the entity assets or annual operating budget.	Limited damage to entity assets or annual operating budget is equivalent to: **a. $10 million to $100 million.**	Damage is: a. substantial financial loss to an entity	Not applicable	Not applicable

[28] The IPPS defines 'personal information' as 'information or opinion, whether true or not, relating to a natural person or the affairs of a natural person whose identity is apparent, or can reasonably be ascertained, from the information or opinion'.
[29] Impacts on an entity or organisation at this scale are considered a matter of national interest.
[30] Impacts on an entity or organisation at this scale are considered a matter of national interest.

			b. $100 million to $10 billion damage to entity assets.		
Legal compliance	Information compromise would not result in legal and compliance issues.	Limited damage is: a. issues of legal privilege for communications between legal practitioners and their clients, or prepared for the purposes of litigation b. contract or agreement non-compliance c. failure of statutory duty d. breaches of information disclosure limitations under legislation resulting in less than two years imprisonment.	Not applicable Impacts on an agency or entity at this scale are considered a matter of state or national interest.	Not applicable Impacts on an agency or entity at this scale are considered a matter of state or national interest.	Not applicable Impacts on an agency or entity at this scale are considered a matter of state or national interest.
Medical patient/ practitioner privilege	Information compromise would not result in compromise to medical practitioner/patient privilege	Limited damage is: a. issues of **medical practitioner/patient privilege** for communications between medical practitioners and their patients b. breaches of information disclosure limitations under legislation.[31]	Not applicable Apply criteria for **dignity or safety of an individual**.	Not applicable Apply criteria for **dignity or safety of an individual**.	Not applicable Apply criteria for **dignity or safety of an individual**.
Aggregated data[32]	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 information that, if compromised, would cause limited damage to the state or 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 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
Sub-impact category: Potential national interest impacts from compromise of the information					
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 business impact level).	Limited damage is: a. impeding the development or operation of policies. b. revealing deliberations or decisions of Cabinet, or matters submitted, or proposed to be submitted, to Cabinet (not otherwise captured by higher level business impacts).	Damage is: a. a. impeding the development or operation of major policies	Serious damage is: a. 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 is: a. a. the collapse of internal political stability of Australia or friendly countries.
Compromise of information would be expected to cause	Not applicable. This is the majority of routine information created or processed by the South Australian public sector, including routine business operations and services. OFFICIAL is not a security classification and compromise would result in no or insignificant damage to individuals, organisation or government.	OFFICIAL information that due to its sensitive nature requires limited dissemination. OFFICIAL: Sensitive is not a security classification. It is a dissemination limiting marker (DLM) indicating compromise of the information would result in limited damage to an individual, organisation or government.	Valuable, important and sensitive information. Compromise of PROTECTED information would be expected to cause damage to the state or national interest, organisations or individuals.	Very valuable, important and sensitive information. Compromise of SECRET information would be expected to cause serious damage to the state or national interest, organisations or individuals.	The most valuable, important and sensitive information. Compromise of TOP SECRET information would be expected to cause exceptionally grave damage to the state or national interest, organisations or individuals.

[31] Relevant South Australian legislation includes: Health Care Act 2008, Mental Health Act 2009, Children's Protection Act 1993. Additional relevant legislation may also be applicable.

[32] 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 have more significant consequences than compromise of individual documents. When viewed separately, the components of the information compilation retain their individual classifications.

Economy	Information from routine business operations and services.	Limited damage is: a. undermining the financial viability of one or more individuals, minor South Australian based or owned organisations or companies b. disadvantaging a major South Australian organisation or company.	Damage is: a. undermining the financial viability of a major South Australian-based or owned organisation or company b. disadvantaging several major South Australian organisations or companies c. short-term material impact on state or national finances or economy.	Serious damage is: a. undermining the financial viability of a South Australian industry sector (multiple major organisations in the same sector) b. long-term damage to the state or national economy to an estimated total in excess of $20 billion.	Exceptionally grave damage is: a. the collapse of the state or national economy.
Infrastructure	Information from routine business operations and services	Limited damage is: a. damaging or disrupting state or territory infrastructure.	Damage is: a. damaging or disrupting significant state or territory infrastructure.	Serious damage is: a. shutting down or substantially disrupting significant national infrastructure.	Exceptionally grave damage is: a. the collapse of all significant national infrastructure.
International relations	Information from routine business operations and diplomatic activities.	Limited damage is: a. a. minor and incidental damage or disruption to diplomatic relations.	Damage is: a. short-term damage or disruption to diplomatic relations b. disadvantaging South Australia in international negotiations or strategy.	Serious damage is: a. severely disadvantaging South Australia in major international negotiations or strategy b. directly threatening internal stability of friendly countries, leading to widespread instability c. raising international tension or severely disrupting diplomatic relations resulting in formal protest or sanction.	Exceptionally grave damage is: a. directly provoking international conflict or causing exceptionally grave damage to relations with friendly governments.
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 of **two 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**[33] b. **affecting the operational effectiveness**, security or intelligence capability of Australian or allied forces.	Exceptionally grave damage is: a. **significantly affecting the operational effectiveness**, security or intelligence operations of Australian or allied forces

[33] Serious organised crime as defined in the Convention Against Transnational Organised Crime.

ANNEX C: TABLE 2 - ALIGNMENT OF CLASSIFICATIONS TO BIL, PROTECTIVE MARKING AND ACCESS REQUIREMENTS

	Sensitive Information		Security Classified Information		
Classification	**OFFICIAL**	**OFFICIAL: Sensitive**	**PROTECTED**	**SECRET**	**TOP SECRET**
Business Impact Level (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 the South Australian public sector	**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	**Optional** **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 (pink) colour marking required**	**Red colour marking required**
Need-to-know	Not required, but recommended	Yes	Yes	Yes	Yes
Valid personnel 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)

ANNEX C: TABLE 3 - MINIMUM PROTECTIONS FOR INFORMATION TRANSMISSION AND TRANSFER

	Sensitive Information		Security Classified Information		
Classification	**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, however: a. secure information in personal custody in a security briefcase or SCEC-approved pouch.	Yes, for official purposes, however: a. subject to agency arrangements for managerial approval. b. Secure information in personal custody in a security briefcase or SCEC-approved pouch.	Yes, **however not recommended**. a. Written, manager-approved record of outgoing material maintained in an auditable log or 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 however: a. in line with agency policies See Minimum protections and handling requirements for OFFICIAL information for more information.	Yes, for official purposes however: a. in line with agency policies b. secure information from unauthorised access. See Minimum protections and handling requirements for OFFICIAL: Sensitive information for more information	Use and storage of information for homebased work is not recommended. See Minimum protections and handling requirements for PROTECTED information for more information.	Use and storage of information for home-based work is not recommended. See Minimum protections and handling requirements for SECRET information for more information.	Not applicable. Use and storage for homebased work is prohibited. See Minimum protections and handling requirements for TOP SECRET information for more information.
Protect information when transferred over public network infrastructure or through unsecured spaces	Yes, for official purposes however, NTK principle **should** be applied	Yes, for official purposes however: a. information **must** be encrypted for transfer over public networks or through Zone One security areas[34]	Yes, for official purposes, however: a. information **must** be encrypted for transfer over public networks or through Zone One security areas [35]	Yes, for official purposes, however: a. information **must** be encrypted for transfer over public networks or through Zone One security areas[36]	Yes, for official purposes however: a. **Must** use High Assurance Cryptographic Equipment encryption for transfer over public networks or outside Zone Five security areas.
Protect information when transferred within a single physical location (e.g., an office)	Yes, for official purposes, however NTK principle **should** be applied	Yes, for official purposes, however NTK principle **must** be applied	Yes, for official purposes, however NTK principle must be applied	Yes, for official purposes, however NTK principle must be applied	Yes, for official purposes, however NTK principle must be applied
Protect information from unauthorised access when transferred between physical establishments in Australia	Yes, for official purposes however, NTK principle **should** be applied	Yes, for official purposes however: a. unauthorised access **must** be deterred, e.g., external mail is sealed.	Yes, for official purposes however: a. **must** be secured from unauthorised access. b. Double enveloping required if SCE Cendorsed courier used.	Yes, for official purposes however: a. must be secured from unauthorised access. b. Double-enveloping and	Yes, for official purposes however: a. must be secured from unauthorised access. b. Double-enveloping and

[34] Encrypt OFFICIAL: Sensitive information transferred over public network infrastructure, or through un-secure spaces, unless the residual security risk of not doing so has been recognised and accepted by the entity. An entity may also wish to consider other security measures or mitigating protections already in place, such as: validating the recipient's address before sending information in an unencrypted form; or sending sensitive information or large amounts of non-sensitive information as an encrypted or password protected attachment.

			c. Receipt required.	i. a security briefcase (or SCEC-approved pouch) and delivered direct by an authorised messenger xi or ii. SCEC-endorsed courier. c. Receipt required.	i. a security briefcase (or SCEC approved pouch) and delivered direct by an authorised messenger xi or ii. safe hand courier c. Receipt required.
Protect information from unauthorised access when transferred between physical establishments outside Australia	Yes, for official purposes however, NTK principle **should** be applied	Yes, for official purposes however: a. unauthorised access **must** be deterred, e.g., external mail is sealed.	Yes, for official purposes however: a. Double enveloping b. Receipt required c. Carriage by DFAT courier service or an authorised officer.[37]	Yes, for official purposes however: a. Double enveloping b. Receipt required c. Carriage by DFAT courier service or an authorised officer.	Yes, for official purposes however: a. Double enveloping b. Receipt required c. Carriage by DFAT courier service or an authorised officer.

[37] An authorised officer is an officer authorised in accordance with the policies of the SAPSF and the agencies procedures

ANNEX C: TABLE 4 - MINIMUM USE AND STORAGE REQUIREMENTS FOR SENSITIVE AND SECURITY CLASSIFIED INFORMATION

	Sensitive Information		Security Classified Information		
Classification	**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 One 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 entity approval required	**Storage** Not to be stored **Use** Not to be used
Zone Two 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: a. originating entity approval required b. SCEC Class A container. **Use** Permitted	**Storage** Not to be stored **Use** Not to be used
Zone Three 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 entity approval and ASIO-T4 advice required b. storage period up to five days in SCEC Class A container **Use** Permitted
Zone Four 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 entity approval and ASIO-T4 advice required b. storage period up to five days in SCEC Class B container **Use** Permitted.
Zone Five No public access. Visitor access only for visitors with a need to know and with close escort. Restricted access for authorised	**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

personnel with appropriate security clearance. Dual factor authentication for access control.					

ANNEX C: TABLE 5 - MINIMUM HANDLING PROTECTIONS FOR DISPOSAL OF SENSITIVE AND SECURITY CLASSIFIED INFORMATION, ICT AND MEDIA EQUIPMENT

	Sensitive Information		Security Classified Information		
Classification	**OFFICIAL**	**OFFICIAL: Sensitive**	**PROTECTED**	**SECRET**	**TOP SECRET**
Destruction of Physical Information					
Use entity-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 cross shredder)	Destroy information by pulping, burning, pulverisation, disintegration, or shredding (Class A cross shredder)	Destroy information by pulping, burning, pulverisation, disintegration, or shredding (Class A cross shredder
Destroyed under supervision of two 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
Destroyed as soon as possible after it has reached the minimum retention period set by State Records of South Australia	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**.		Not applicable	Not applicable	Destroy information as soon as possible
SA CABINET caveated material	Not applicable. **SA CABINET** caveat must not be used at this classification.	As per requirements of the SA Cabinet Handbook	Destroy information by pulping, burning, pulverisation, disintegration, or shredding (Class B cross shredder)		Destroy information by pulping, burning, pulverisation, disintegration, or shredding (Class A cross shredder)
Destruction of ICT media and equipment					
Undergo media sanitisation or destruction in accordance with South Australian Cyber Security Framework	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 media and equipment	Sanitise or destroy ICT media and equipment	Sanitise or destroy ICT media and equipment
Destroyed as soon as possible after it has reached the minimum retention period set by State Records of South Australia	Not applicable. While all official information must be disposed of securely, there is no minimum requirement for how to dispose **OFFICIAL** or **OFFICIAL: Sensitive information**		Not applicable	Not applicable	Destroy information as soon as possible

Government
of South Australia