South Australian Information Classification System overview

Description

1. The South Australian Information Classification System (ICS) commenced on **1 December 2019**. The ICS is used to assist South Australian public sector agencies[i] to assess the confidentiality, integrity and availability of their information assets and ensure the appropriate protections, including protective markings and handling requirements, are assigned. The ICS replaces the classifications previously outlined in the Information Security Management Framework (ISMF).

2. Agencies have a one-year transition period (until **1 December 2020**) to implement the ICS. During this period both the ICS and ISMF classification systems and associated protective markings will be recognised, after which, the ISMF classifications and protective marking will cease to be recognised. Guidance material and resources have been developed to support agencies to implement the ICS and associated information security requirements (see **Resources**).

3. The ICS is based upon the Commonwealth Government's sensitive and classified information requirements under the Protective Security Policy Framework (PSPF) with some modifications to suit the South Australian context.

4. The ICS, and accompanying policy and guidance forms a part of the information security requirements of the **South Australian Protective Security Framework** (SAPSF).

5. This document provides a high-level outline of the ICS, including classifications and protective markings for use in the South Australian Government.

[i] The ICS applies to all South Australian public sector agencies (as defined in 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".

Classifications

6. Information produced within the South Australian Government creates an official records of government actions and decisions. Official records must be appropriately protected to prevent damage from intentional and accidental threats. Assessing the business impact or 'damage' that may occur from compromise[ii] of official information enables agencies to apply the appropriate classification.

7. Classification enables agencies to protect their information in a consistent, organised and appropriate way. The following classifications have been approved for use in the South Australian Government.

UNOFFICIAL	**UNOFFICIAL** can be used for non-work-related information (including emails). Use of the protective marking is optional.
OFFICIAL	**OFFICIAL** describes routine information created or processed by the South Australian public sector with a low business impact. Use of the protective marking is optional, but **recommended**.
OFFICIAL: Sensitive[iii]	**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**.
PROTECTED[iv]	**PROTECTED** is a security classification which indicates that compromise of the information may result in **damage** to the state or national interests, organisations or individuals. Use of the protective marking is **mandatory**.
SECRET[iv]	**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[iv]	**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**.

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

[iii] Examples of **OFFICIAL: Sensitive** information **may** include:

a. 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.
b. commercial or economic data that, if compromised, would undermine a South Australian organisation or company, and/or provide an unfair economic advantage.
c. information that, if compromised, would impede development of government policies.

[iv] 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.

Caveats and accountable material

8. A caveat is a warning that the information contained has special protections *in addition to* those indicated by the classification. Types of caveats which may be encountered in South Australian include sensitive compartment information (codewords), foreign government markings, special handling instructions or releasability caveats.

9. Caveats **must** only be used *in addition to* the classification protective marking.

10. Accountable material[v] is information requiring stricter control over its access and movement. This includes select special handling instruction caveats (e.g. SA Cabinet information), codeword information, and any other information designated as accountable by the originator.

11. All agencies are responsible for protecting caveated and accountable material in accordance with the access and handing requirements assigned by the originator.

SA Cabinet caveat

12. South Australian Cabinet information is considered accountable material requiring certain protections to be in place over and above those afforded by the classification. As such, the ICS has introduced a **SA CABINET** caveat to replace the previous 'Sensitive: SA Cabinet' DLM.

13. **SA CABINET** is a 'special handling instruction' caveat which restricts access to Cabinet information to only those with an identified need to know, and who are appropriately security cleared (if required by the classification). The caveat's handling instructions will apply *in addition to* any classification handling instructions.

14. The **SA CABINET** caveat identifies any material that:

    a. is prepared for the purpose of informing the South Australian Cabinet

    b. reveals the decision 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 considred by the South Australian Cabinet.

15. *The* **SA CABINET** *caveat* ***must*** *only appear in addition to the assigned classication*. The ICS requires that all South Australian Cabinet material has a classification of **OFFICIAL: Sensitive** or higher.

Examples:

OFFICIAL: Sensitive//SA CABINET

PROTECTED//SA CABINET

Other caveats

16. Other caveats that may be encountered in South Australia include:

[v] accountable material may vary from entity to entity and could include budget papers, tender documents and sensitive ministerial briefing documents.

a. **EXCLUSIVE FOR (named person)** – access is limited to a named person, position title or designation and minimum classification of **OFFICIAL: Sensitive** **must** be applied.

b. **AUSTEO, AGAO & REL** – these are releasability caveats which limit access based on citizenship. They are used only with information classified at **PROTECTED** or above. Additional information on their use is found in SAPSF policy **Protecting official information.**

Information Management Markers

17. The ICS provides agencies with optional information management markers (IMMs) which can be used to help identify information which may have legislative or professional restrictions. They take the place of the former suite of DLMs.

18. The IMMs are **not** classifications and **must** only be used in addition to an appropriate classification of **OFFICIAL: Sensitive** or higher.

19. It is important to note that the IMMs do not provide any greater level of protection than the classification and are intended for information management purposes where disclosure of the content would breach specific legislative or professional restrictions.

20. The following table contains the IMMs under the ICS.

South Australian Information Management Markers (IMM)

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 legislative secrecy provisions
Personal privacy	Restrictions, under Premier's Circular PC012 - Information Privacy Principles (IPPS) Instructions, on access to, disclosure of, or use of, personal information collected or received
Medical in confidence	Restrictions on access to, or use of, information covered by medical practitioner/patient privilege, or legislative disclosure restrictions

Examples:

OFFICIAL: Sensitive//Medical in confidence

SECRET//AUSTEO//Legal privilege

Protective markings

21. Protective markings notify users and systems that the information requires some level of protection. They are easily identifiable for users (as a visual mark) and for systems (e.g. agency's email gateway) to help to control the distribution of information.

22. The types of protective markings and their order of precedence is as follows:

    a. classification

    b. foreign government information markings (if any)

    c. caveats or other special handling instructions (if any) then

    d. information management markers (optional, if any).

23. As multiple protective markings can be applied to a piece of information, a double forward slash (***//***) **should** be used to help to clearly differentiate each marking.

24. Text-based markings are the preferred method to identify sensitive or security classified information. Text-based protective markings **should** be**:**

    a. in capitals, in a large, plain text font, in a distinctive colour (red preferred)

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

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

Examples:

OFFICIAL: Sensitive//Personal privacy

PROTECTED//SA CABINET

25. Where text-based markings cannot be used (e.g. certain media or assets), colour-based markings are required. See SAPSF policy ***Protecting official information*** for more information.