STATE EMERGENCY MANAGEMENT PLAN

CLASSIFICATION AND RETENTION OF EMERGENCY MANAGEMENT PLANS AND OFFICIAL INFORMATION

PART 3: GUIDELINES AND FRAMEWORKS

Government of South Australia

STATE EMERGENCY MANAGEMENT PLAN (SEMP)		
Part 1 Arrangements	Part 2 Strategies, Guidelines and Frameworks	Part 3 Supporting Plans
Governance arrangements, roles and responsibilities, and structures in place to reduce risk from hazards, and to plan and prepare for, respond to and recover from emergencies.	Various strategies, guidelines and frameworks that support the state's emergency management arrangements.	Required plans that support the state's emergency management arrangements (including hazard risk reduction plans, capability plans, control agency plans, functional support group plans, zone emergency management plans and operations manuals).

Figure 1: The SEMP is a series of documents split over 3 parts with accompanying annexes. This guidelines sits under Part 2 of the SEMP.

The Classification and Retention of Emergency Management Plans and Official Information Guideline can be found at: https://www.dpc.sa.gov.au/responsibilities/security-emergency-and-recovery-management/state-emergency-management-plan

The custodian of the Classification and Retention of Emergency Management Plans and Official Information Guideline is the State Emergency Management Committee (SEMC) who may delegate this responsibility to a sub-committee of SEMC.

CONTENTS

1. CLASSIFICATION AND RETENTION OF EMERGENCY MANAGEMENT PLANS AND OFFICIAL INFORMATION

Introduction

These paragraphs outline how agencies will classify and retain emergency management official Information. These instructions comply with the South Australia Government South Australian Information Classification System (ICS) and the State Records General Disposal Schedule 33 (GDS). The ICS, and accompanying policy and guidance forms a part of the information security requirements of the South Australian Protective Security Framework (SAPSF).

The South Australian Information Classification System provides detailed and extensive information to assist South Australian public sector agencies 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).

To protect emergency management official information against compromise, agencies[1] 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] 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".

Further information can be found in the South Australian Protective Security Framework's Information Security policies https://www.security.sa.gov.au/protective-security-framework/information-security.

Classifications

The South Australian Information Classification System describes the following classifications that 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[2]	**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	**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	**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	**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**.

It is typically considered appropriate that emergency management plans and other official documents are classified as either Official or Official: Sensitive. As such, this annex does not outline the requirements in relation to Security Classified Information being Protected, Secret and Top Secret information.

Caveats and accountable material

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 Australia include sensitive compartment information (codewords), foreign government markings, special handling instructions or releasability caveats.

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

[2] 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.

Accountable material[3] 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.

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

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.

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

a. is prepared for the purpose of informing the South Australian Cabinet and the Emergency Management Cabinet Committee (EMCC)

b. reveals the decision and/or deliberations of the South Australian Cabinet and the EMCC

c. is prepared by departments to brief their Ministers on matters proposed for South Australian Cabinet and the EMCC consideration

d. has been created for the purpose of informing a proposal to be considered by the South Australian Cabinet and the EMCC.

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

Protective markings

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.

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.

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)

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

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//SA CABINET

See SAPSF policy ***Protecting official information*** for more information.

Classification of Emergency Management Plans and Official Information

Table 1: Classification for Emergency Management official information.

Document	Classification
Emergency Management Plans	
Draft Version Emergency Management Plans	Official: Sensitive
State EM Plan	Official
SEMP Part 1, 2, 3	Official
SEMP Part 2 annexes	Official
Hazard Risk Reduction Plan	Official or Official: Sensitive
Functional Support Group Plan	Official or Official: Sensitive
Capability Plan	Official or Official: Sensitive
Control Agency Plan	Official or Official: Sensitive
Zone EM Plan	Official or Official: Sensitive
Committee minutes	
State EM Committee	Official: Sensitive
SEMC Sub-committees (and Working Groups)	Official: Sensitive
Zone EM Committees	Official: Sensitive
Zone EM Sub-committees	Official: Sensitive

The marking of other emergency management information should suitably reflect the importance, degree of sensitivity and protection requirements using the choices outlined the South Australian Information Classification System.

Retention of Emergency Management Plans and Official information

As per the requirements of the State Records Act, General Disposal Schedule 33 (GDS33) “Across Government Emergency Management” has been prepared to describe the retention requirements of all emergency management documentation. GDS 33 defines the Responsible Records Agency as

"the South Australian Government Agency that provides the role of either Chair and or Executive Officer to a committee or function, or the South Australian Government Agency that prepares or manages a plan or document pursuant to the Emergency Management Act. Where a committee or function is chair by a Commonwealth Government organisation or private entity, the nominated South Australian Government Agency represented on that committee or function is the Responsible Records Agency"

The Responsible Records Agency (RRA) is required to maintain a full and accurate copy of all records as per GDS33 and comply with the State Records Act storage and retention requirements. Other agencies that have identical records (i.e. unaltered copies) are no longer required to retain them permanently.

Where an agency prepares further papers to support the key documents, e.g. briefing notes, executive briefings etc, those papers must be kept in line with the requirements of GDS 33 (i.e. the same as the RRA), but not the originating papers.

Full details of record classes/types are contained within GDS33 available from State Records of South Australia.

The below table lists Responsible Record Agencies for various record types. Where the below table is inconsistent with GDS 33, then GDS 33 will apply

Table 2. Responsible Records Agencies.

Document	Responsible Records Agency
Emergency Management Plans	
Draft Version Emergency Management Plans	Authoring agency
State Emergency Management Plan	Department of Premier and Cabinet
SEMP Support Plan	Authoring Agency
State Controller Contact Details	Department of Premier and Cabinet (as part of SEMC Papers)
Hazard Risk Reduction Plan	Hazard Risk Reduction Leader
Functional Support Group Plan	Lead agency
Capability Plan	Lead agency
Control Agency Plan	Lead agency
Zone Emergency Management Plan	Zone Executive Officer (State Emergency Service)
Committee Minutes and supporting Papers, Agenda's etc	
State Emergency Management Committee (SEMC)	Department of Premier and Cabinet

Document	Responsible Records Agency
SEMC Sub-committees	Chair of each committee (where SA Government)
Working groups and committees	Chair of working group or committee (where SA Government)
Zone Emergency Management Committees	Zone Executive Officer (State Emergency Service)
Zone Emergency Management Sub-committees	Zone Executive Officer (State Emergency Service)
National Committees (eg ANZEMC and subcommittees)	Senior SA Government Representative (ie Department of Premier and Cabinet where present)

Document Control Page

A Document Control Page shall be used for Emergency Management Plans and shall be located after the document cover sheet and before the table of contents section, or at the back of the document.

Secure Web-based Portals

Microsoft Teams and the Australian Government's GovTeams provide secure web-based spaces designed to facilitate business collaboration across policy portfolios and administrative jurisdictions. Both portals can be accessed remotely via the web by any persons with a security password. The State Emergency Management Committee has approved the use of the Microsoft Teams SA Emergency Management Site and the Australian Government's GovTeams to host emergency management official information that is shared across government.

South Australian emergency management official information that is shared across the state government is hosted on the Microsoft Teams SA Emergency Management site. Information relating to national committees and national EM matters (e.g. ANZEMC and subcommittees) that is shared across government is hosted on GovTeams. Both portals are accredited to hold information up to and including the Official: Sensitive classification, however, any Official: Sensitive documents marked with the SA Cabinet caveat should not be hosted on these portals.

IT IS IMPORTANT TO NOTE that Microsoft Teams and GovTeams will not be available during power outages, network failures or system upgrades from several hours up to several days. It is therefore not a reliable sole source repository for Official: Sensitive information for which there is at least a moderate availability requirement (the loss would have a significant impact and recovery must be achieved within a period measured in days – typically three business days or less).

Official documents noted in Table 1 as Official: Sensitive for which there is an absolute availability requirement (the loss would be crippling and recovery must be virtually instantaneous – no longer than a few minutes), will be maintained on the Microsoft Teams Emergency Management site, the State Emergency Centre Registry computer and copies within SAPOL Emergency and Major Event Section to ensure availability requirements.

All agencies must ensure that they have alternative retrieval processes other than MS Teams or GovTeams for documents classified in Table 1 as Official: Sensitive for which there is at least a moderate availability requirement (the loss would have a significant impact and recovery must be achieved within a period measured in days – typically three business days or less).

Aggregation of Information

The use of the Microsoft Teams and GovTeams will result in aggregation of official Information. Access to information is to be restricted according to the document DLM and caveat.

2. GLOSSARY

Term	Definition
ICS	Australian Information Classification System
ANZEMC	Australia-New Zealand Emergency Management Committee
GDS33	General Disposal Schedule 33
ISMF	Information Security Management Framework
RRA	Responsible Records Agency
SAPSF	South Australian Protective Security Framework
SEMC	State Emergency Management Committee
SEMP	State Emergency Management Plan

3. DOCUMENT CONTROL

Version	Draft Version 2.0
Classification	Official
Authority	State Emergency Management Committee pursuant to Section 9(1)(b) of the *Emergency Management Act 2004* (SA)
Managed and maintained by	The Department of the Premier and Cabinet
Review cycle	Biennial review
Issued	16 December 2016
Scheduled review date	2 March 2025
Disclaimer	Users should ensure that they have the current version before taking action based on this plan

Version	Date	Summary of change
1	16 December 2016	Version 1
2	17 February 2023	Version 2 includes significant updates to classifications and caveats to reflect the replacement of the Information Security Management Framework with the South Australian Information Classification System. References to Govdex have been replaced with new portals. Availability requirements updated.

Government
of South Australia