South Australian Protective Security Framework

INFOSEC2:

Accessing official information

SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK

Contents

SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK

Purpose

1. This policy ensures all South Australian Government agencies provide timely, reliable and appropriate access to official information to assist in facilitating efficient and effective delivery of government services. Availability of accurate information aides in the development of new products and services, enhances consumer and business outcomes and assists with decision-making and policy development.

Core Requirement 8

Ensure official information is available to those who need it.

Supporting Requirements

2. To ensure official information is available to those who need it, agencies[1] **must:**

   I. ensure information is accessed only by personnel with a legimate need-to-know

   II. ensure personnel requiring ongoing access to sensitive information have undertaken the appropriate pre-employment screening checks

   III. ensure personnel requiring ongoing access to security classified information have the appropriate security clearance[2] and meet any additional suitability requirements[3]

   IV. put in place an agreement or arrangement[4] to enable sensitive or security classified information to be shared with personnel or organisations outside of the South Australian Government

   V. manage access to information systems by implementing unique user identification, authentication and authorisation practices for each approval of system access

   VI. ensure temporary access to security classified information is strictly controlled according to the requirements of this policy

[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".

[2] Some office holders are not required to hold a security clearance. See **Security clearance exemptions** for the full list.

[3] Some caveats or codeword information **may** impose additional requirements on the individual *in addition to* the security clearance. Please refer to PSPF policy Access to information for more detail.

[4] Such as a contract or deed which outlines how the information is to be used and what protections **must** be applied.

SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK
Terminology

Term	Meaning
MUST	Use of the word must (or required) indicates a mandatory requirement or action of the policy to which all agencies must adhere or undertake.
MUST NOT	Use of the words must not indicates an action prohibited by this policy.
SHOULD	Use of the word should (or recommended) indicates an action that agencies ought to undertake, unless prevented by legitimate circumstances or justification.
SHOULD NOT	Use of the words should not (or not recommended) indicates an action which agencies should avoid, unless legitimate circumstances prevent another course of action being taken.
MAY	Use of the word may indicates an action which is completely optional, but may be provided as a suggestion or considered best practice.

Definitions

Term	Definition
agency	as per the definition of *public sector agency* (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”.
agreement or arrangement	a document, such as a contract or deed, which outlines how the information is to be used and what protections **must** be applied
availability	allowing authorised persons to access information for authorised purposes at the time they need to do so
biometrics	the technical term for body measurements and calculations – it refers to related human characteristics
classification	an indication of the level of protection information needs to prevent compromise (for example **OFFICIAL: Sensitive**)
caveat	a warning (such as protective marking) which indicates the information has additional protections required in addition to those indicated by the caveat.
compromise	includes, but not limited to, loss, misuse, interference, unauthorised access, unauthorised modification, unauthorised disclosure.
handling	any processes for accessing, transmitting, transferring, storing or disposing of, official information
originator	entity or individual that initially generated and/or is responsible for the information (also owner)
personnel	all people that an agency employs (including contracted employees)
protection	the steps taken to maintain the confidentiality, integrity and availability of official information
sensitive	indicates information requires *some* level of protection but is not security classified
visitor	any person who is not an agency employee with ongoing access to agency facilities

Term	Definition
suitability	the combination of eligibility and fit for the role, assessment of integrity and ability to meet the assessment criteria or other requirements

Acronyms

Acronym	Words
AGSVA	Australian Government Security Vetting Agency
ICS	South Australian Information Classification System
ICT	Information Communication Technology
IPPS	Premier's Circular PC012 Information Privacy Principles Instructions
MFA	Multi-factor authentication
NTK	Need-to-know principle
PSPF	Protective Security Policy Framework (Commonwealth)
SACSF	South Australian Cyber Security Framework
SARKMS	South Australian Recordkeeping Metadata Standard
SMSMP	Sensitive Material Security Management Protocol

SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK
Guidance

Applying the need-to-know principle

3. The need-to-know (NTK) principle reflects the need for personnel to only access information where there is an operational need to do so. Applying this principle to agency information security practices helps personnel to understand their responsibilities to protect information from compromise.
4. NTK works to reduce unauthorised access to, and potential compromise of, relevant official information, whilst also enabling positive information sharing between people where an operational benefit would be derived.
5. Access to sensitive and security classified information **must** be limited to authorised personnel whose responsibilities require access to that information. Access **must not** be given based upon convenience, an individual's status, position, rank or level of authorised access.

Pre-employment screening checks

6. Personnel who have a requirement for ongoing access to sensitive information (**OFFICIAL: Sensitive**) **must** undertake appropriate pre-employment screening checks. The list of **required** and **recommended** pre-employment screening checks can be found under SAPSF policy Recruiting employees.
7. Agencies are **responsible for** ensuring their satisfaction that their employees meet all the identified suitability requirements.

Security clearance and suitability requirements

8. In addition to NTK, personnel requiring ongoing access to security classified information **must** have a valid security clearance at the appropriate level. **Table 1 – Minimum security clearance levels for ongoing access to information** lists the required security clearance for each level of classification.

Table 1 – Minimum security clearance levels for ongoing access to information

UNOFFICIAL	Not applicable.
OFFICIAL	Security clearance not required. Appropriate pre-employment screening is sufficient.
OFFICIAL: Sensitive	Security clearance not required. Appropriate pre-employment screening is sufficient.
PROTECTED	**Baseline** security clearance or above.
SECRET	**Negative Vetting 1** security clearance or above.
TOP SECRET	**Negative Vetting 2** security clearance or above.

Security clearance exemptions

9. Some Australian office holders are not required to hold a security clearance to access security classified information while exercising the duties of the office. Australian office holders who do not need a security clearance are:

a. Members and senators of the Commonwealth, state parliaments and territory legislative assemblies
b. Judges of the High Court of Australia, the Supreme Court, Family Court of Australia, the Federal Circuit Court of Australia, and magistrates
c. royal commissioners
d. the Governor-General, state governors, Northern Territory administrator
e. members of the Executive Council
f. appointed office holders with enabling legislation that gives the same privileges as the office holders already identified e.g. members of the Administrative Appeals Tribunal.

10. Staff of the office holders above are not exempt from the security clearance requirements.
11. For information regarding personnel security clearance assessments, see the PSPF policy: Eligibility and suitability of personnel.

Caveated information

12. Caveat owners **may** impose additional access or suitability requirements on top of the classification. Personnel accessing caveated information **must** meet all clearance and suitability requirements imposed by the originator.
13. SAPSF policy Protecting official information provides guidance on caveats that **may** be encountered in the South Australian Government.
14. The **SA CABINET** caveat requires that all personnel accessing information bearing that caveat **must** sign a SA Cabinet Confidentiality Agreement. Further information can be found in the SA Cabinet website.[5]
15. Some caveats limit access based on citizenship. The releasability caveats **AUSTEO** (Australian Eyes Only), **AGAO** (Australian Government Access Only) and **REL** (Releasable to) preclude certain people from accessing that information or material.
16. Agencies **must not** share information caveated **AUSTEO** with a person **who is not** an Australian citizen (dual citizenship **does not** preclude access). If there is a business need to share **AUSTEO** caveated information with a non-citizen, the owner **may** reconsider applying the caveat or amending the classification (see SAPSF policy INFOSEC1: Protecting official information).
17. Similarly, **AGAO** **must not** be shared with a person who is not an Australian citizen.[6]

Information sharing agreements

18. Access to, and use of, official information can be necessary for an external entity's[7] operations, however, additional risks arise from sharing official information externally of government.
19. Because the SAPSF and associated requirements apply only to South Australian public sector agencies, external entities may not apply commensurate information security policies or practices. As a result, in incidents of information compromise, there may be limited options for recourse or recovery.

---

[5] Handling and protection requirements for Commonwealth caveated information are not all publicly available. The Sensitive Material Security Management Protocol (SMSMP) sets out the protection and handling requirements for caveated information. The SMSMP is available to entity security advisors via GovTeams.

[6] **AGAO** material is releasable to appropriately cleared representatives of Five-Eyes foreign governments on exchange or long-term posting to Australian Intelligence Community agencies.

[7] External entities **may** include non-governmental organisations (NGOs), contractors or service providers and **may** include individuals or organisations.

20. As such, this policy requires that all agencies **must** put in place a formal, legally binding, written agreement, such as a contract or deed, with external entities with whom they share, or may share, sensitive or security classified information.

21. Such an arrangement **must** ensure the external entity understands the obligations to protect government information to the same standard as outlined in the SAPSF, and that use of the information is not inconsistent with the Information Privacy Principles (IPPS) Instruction.

Managing access to information

22. A well-structured, robust ICT system provides personnel the right tools and access to effectively undertaken their work. It also assists to protect information, systems and intellectual property from compromise.

23. Access to networks, operating systems, applications and information **should** be controlled by:

    a. establishing a clear understanding of the information held on such systems
    b. effective user identification and authentication practices.

24. For guidance on ICT system development, see the SAPSF policy Robust ICT and cyber security.

User identification, authentication and authorisation practices

User identification and authentication

25. All agencies **should** know who is accessing their information and when. To mitigate unauthorised or inappropriate access to and use of official information, agencies **must** establish formal user registration and de-registration procedures for granting and revoking access to information systems.

26. All users **must** be authenticated on each occasion they seek access to information systems. Establishing uniquely identifiable user processes ensures a greater degree of accountability that information is being access appropriately.

27. Methods to authenticate access include:

    a. passphrases (preferred) or passwords[8]
    b. biometrics
    c. cryptographic tokens
    d. smart cards

28. Agencies **may** reduce the risk of unauthorised access or compromise by:

    a. using multi-factor authentication (MFA - two or more authentication methods) where users provide something they know (e.g. passphrase/password), something they have (e.g. physical token) and/or something they are (e.g. biometrics)
    b. increasing the complexity of single authentication methods (passphrases/passwords) by increasing the minimum length and use of alphanumeric and special characters.

29. Agencies **should** regularly review user access rights to provide confidence that access to sensitive or security classified information is for authorised purposes only.

[8] The Australian Cyber Security Centre provides advise on improving password security at Get smarter with passwords

High-risk users

30. Some users or system access incur a greater level of risk, such as system or network administrators and managers, database administrators, privileged users (and other similar positions of trust) and remote access users.

31. System and network managers, for example, have a high-degree of trust placed upon them to both enable appropriate access to information while protecting and not misusing their own privileged access.

32. High-risk users **should** use MFA to ensure their identity on each occasion system access is granted.

Authorising access to ICT systems

33. Robust authorisation processes help agencies to effectively control access to their ICT systems, networks, (including remote access), infrastructure and applications. Agencies **should** implement processes to manage authorised access to systems holding sensitive and security classified information. **Table 2 – Recommended access authorisation measures**outlines the recommended access authorisation measures.

Table 2 – Recommended access authorisation measures[9]

Type of access authorisation	Recommended process
User access management	Ensure systems for managing passwords are interactive and require users to follow good security practices in the selection and us of passwords or passphrases.
Authorised network access	Consider the user of automatic equipment identification as a means to authenticate connections from specific locations and equipment. Control physical and logical access to diagnostic and configuration ports. Restrict the ability of users to connect to shared networks, including those that extend across agency boundaries. Segregate groups of information services, users and information systems, based on an agency risk assessment. Implement routing controls for networks to ensure computer connections and information flows do not breach other relevant access management measures.
Authorised operating system access	Control access to operating systems through a secure log-on procedure. Restrict and tightly control the use of utility programs that may be capable of overriding system and application controls. Display restricted access and authorised use only (or equivalent) warnings upon access to all agency ICT systems, and shut down inactive sessions after a defined period of inactivity. Consider restricting connection times to provide additional security for high risk applications.
Application and information access	Afford sensitive systems a dedicated (isolated) computing environment, in accordance with agency risk assessment.
Mobile computing and communications	Adopt security measures to protect against the risks of using mobile computing and communications facilities.

[9] Please refer to the **SACSF** for more detailed information on how to implement these measures.

SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK

Temporary access to security classified information

34. Temporary access to security classified information up to **SECRET** without a security clearance can be permitted under strict circumstances where the correct risk assessment has been completed.
35. Temporary access **may** include:
    a. short-term[10] where the person does not hold a valid security clearance, but can demonstrate a valid need-to-know, and the risks can be adequately mitigated. This **may** include, but is not limited to:
        i. new starters
        ii. people on short, fixed-term projects
        iii. people who are reasonably expected to only have incidental or accidental contact with security classified information (e.g. security guards, cleaners, external IT personnel, or visitors who do not have an ability to comprehend the classified information[11])
    b. provisional access[12], where the person has commenced a clearance process by providing the relevant details for assessment by a vetting agency. The type of temporary access can be changed from short-term to provisional once the vetting agency has confirmed that the completed security clearance pack has been received and advises the agency that no initial concerns have been identified.
36. All temporary access **must** be supervised, including:
    a. escorting visitors in premises where classified information is stored or used
    b. management oversight of the work of personnel with temporary access
    c. monitoring and auditing incidents of contact with security classified information[13].
37. Temporary access to **TOP SECRET** information **must not** be given unless the personnel seeking access holds an existing Negative Vetting 1 security clearance.
38. Temporary access to caveated information **must** only be granted where all suitability requirements are also satisfied.

Risk assessment for temporary access

39. When assessing risk for temporary access to security classified information, agencies **should** include the following considerations:
    a. the need for temporary access – can the need be filled by someone already holding the necessary clearance?
    b. confirmation from AGSVA or another authorised vetting agency that the person has no identified security concerns, or has ever had a clearance cancelled or denied
    c. what consequences arising from compromise to the information could cause
    d. how that access will be supervised and/or audited
    e. other risk mitigations, such as pre-employment screening checks, character assessments and/or knowledge of personal/work history.
40. The originator or owner of the security classified information **should** be notified, and agreement sought to make the information available.

---

[10] Short-term is considered a maximum of three (3) months in a 12-month period.
[11] This is considered to be children under 10 years of age.
[12] Provisional access **may** be granted to personnel up until a clearance application is granted or denied.
[13] Monitoring and audit logging (d related audit trails) are key measures to control access to ICT systems and the information held on those systems. For further information about developing and maintaining robust ICT systems SAPSF policy Robust ICT and cyber security.

41. Confidentiality or non-disclosure agreements **may** be appropriate to reinforce all requirements to protect the information.
42. Temporary access to caveated information must be approved by the caveat owner based upon a risk-assessment considering compromise of that information.

Document control

Approved by: Jim McDowell	Title: Chief Executive, Department of the Premier and Cabinet
Contact person: James Doherty	Telephone: 0447 180 915
Division: Security and Emergency Management, International and Diplomatic Relations	Date of approval: 25 November 2019
Revision number: 1.2	Date of review: 21 August 2020
Next review date: December 2021	

Change Log

Version	Date	Changes
1.0	25/11/2019	First issue of policy
1.1	20/04/2020	- Classification protective marking examples changed to red colour - Removal of word 'your' throughout entire document
1.2	21/08/2020	- Supporting requirement V(a) moved to SAPSF policy **INFOSEC1: Protecting official information** - Definitions for 'personnel' and 'visitor' added. - Additional guidance added to Caveated information (paras 15-17)