SACSF/G6.0

GOVERNMENT GUIDELINE ON CYBER SECURITY

SACSF Guideline – Integrity and Availability Classification using the SACSF

Purpose

Cyber security is fundamental to the successful operations of the South Australian Government (SA Government). The South Australian Cyber Security Framework (SACSF) has been prepared to standardise and guide the approach for establishing, implementing, maintaining and continually improving the cyber security posture of SA Government agencies.

This guideline is intended to support agencies to implement a process for classifying the integrity and availability requirements of information assets (including ICT systems, platforms, services, applications, and facilities). This enables an agency to appropriately plan, resource and maintain effective information security controls in line with classification requirements.

Refer to the *South Australian Information Classification System (ICS)* for mandated information confidentiality classifications.

Scope

The SACSF applies to:

- South Australian Government public sector agencies, that is, administrative units, bodies corporate, statutory authorities and instrumentalities of the Crown as defined in the *Public Sector Act 2009*.
- Suppliers to the SA Government and non-government personnel provide services to agencies.

The SACSF and the South Australian Protective Security Framework (SAPSF) detail the importance of classifying information and associated information assets (such as ICT systems) based on confidentiality, integrity and availability.

The SAPSF policies that align with this guideline include:

- **INFOSEC1: Protecting official information** - Protect the agency's information against compromise.

The SACSF policy statements that align with this guideline include:

- **SACSF Policy Statement 2.1: Information Asset Identification and Classification** - Information assets supporting critical processes must be identified, recorded and classified. Processes must be place for labelling, storing, handling and disposing of assets in alignment with their classification. Agencies must comply with SACSF Ruling 2 – Storage and Processing of information in outsourced or offshore ICT arrangements.

Guideline detail

SA Government classification schemes

Confidentiality classifications are described in the SAPSF *South Australian Information Classification System (ICS)*.

The following tables describe the integrity and availability classifications.

Using these descriptions, information owners can appropriately classify ICT systems based on the integrity and availability requirements of the information held. The process recognises that information for the public may require exceptionally high degrees of integrity (accuracy) and availability.

Integrity classification scheme

Classification	Description
I4	**ABSOLUTE** requirement, implying that no inaccuracies or omissions can be tolerated.
I3	**HIGH** requirement, meaning that a loss of integrity would cause significant embarrassment and disruption and might be difficult to detect.
I2	**MODERATE** requirement, meaning that the Agency would be somewhat affected by a loss of integrity, but the situation could be easily detected and recovered.
I1	**LOW** requirement, such that there would be minimal impact if the data was inaccurate or incomplete.

When applying an **integrity** classification to an information asset consider the following:

- How accurate must the information be?
- What inaccuracies to the information can be tolerated prior to undertaking corrections or reissuing the information?
- What are the consequences if the information contains errors, becomes corrupted or de-faced or contains omissions?

Availability classification scheme

Classification	Description
A4	**ABSOLUTE** requirement, meaning that the business would be crippled by the loss and recovery must be virtually instantaneous (no longer than a few minutes).
A3	**HIGH** requirement, meaning that loss would cause major disruption to the business and recovery must be achieved within a period measured in hours (typically same business day).
A2	**MODERATE** requirement, implying the loss would have a significant impact and recovery must be achieved within a period measured in days (typically three business days or less).
A1	**LOW** requirement, meaning that loss of the data would have only a minor impact on the business for an extended period (i.e. “best-effort” recovery).

When applying an **availability** classification to an information asset consider the following:

- What is the tolerable outage for the information?
- How dependent is the business unit, the department, clients or the community on this information asset?
- What are the business impacts a disruption or loss of access to the information may cause?

Considerations

Agencies should conduct information asset classifications to classify the confidentiality, integrity and availability requirements for all ICT systems.

- Embed the requirement to conduct an information asset classification for all new systems, and when major changes occur, into policies and procedures.
- Classify agency ICT systems using a documented information asset classification procedure.
- Record the details in an information asset register. The confidentiality, integrity and availability for all ICT systems should be recorded in an information asset register and stored securely.

The information asset register should include at a minimum:

- system name
- information owner, contact details and position
- date of information asset classification approval
- information asset classification review date
- whether the system supports business critical processes
- confidentiality, integrity and availability classifications.

The information asset register may also include:

- if the system is supported by a supplier, and supplier contact details
- whether the system holds personal information.

Protection efforts should be prioritised for assets and information that are considered critical to the ongoing operations of the agency.

Cyber security risk assessments and security control recommendations should reflect the information asset classification of the system.

Additional considerations

Information owners should contact their agency Information Technology Security Adviser (ITSA) for further advice and guidance on agency specific classification procedures and guidelines.

The individual requirements and operational characteristics of agencies will have direct bearing on what measures are implemented to mitigate identified risk(s) and how such outcomes are achieved.

Aboriginal Impact Statement

The needs and interests of Aboriginal people have been considered in the development of this guideline. There is no specific impact on Aboriginal people.

Related documents

- South Australian Cyber Security Framework (SACSF)
- South Australian Protective Security Framework (SAPSF)
- PC030 Protective Security Management Framework
- PC042 Cyber Security Incident Management

Definitions

Term	Definition
Availability	The assurance that systems and information are accessible and useable by authorised entities when required
Information Asset	Any information or asset supporting the use of the information that has value to the agency, such as collections of data, processes, ICT, people and physical documents.
Information Owner	The individual or group responsible and accountable for a set of information. The information owner may, at their discretion, assign responsibility for management of the information to another person or group, also known as an information custodian.
Integrity	The assurance that information has been created, amended or deleted only by authorised individuals.
Business critical processes	Agency processes that, if not performed, would eventuate in the highest level of risk to the agency. This could include meeting critical needs of the agency or satisfying mandatory regulations and requirements.

Acronyms

Acronym	Words
SACSF	South Australian Cyber Security Framework
ICS	South Australian Information Classification Scheme

DOCUMENT CONTROL

Approved by: CIO Steering Committee	
Contact: Chief Information Security Officer	
Division: Office of the Chief Information Officer	Compliance: Optional
Review number: V1.2	Date of approval: 29 August 2023
Next review date: August 2024	Original approval date: November 2019

Licence