SACSF/G6.0

GOVERNMENT GUIDELINE ON CYBER SECURITY

# SACSF Guideline – Integrity and Availability Classification using the SACSF

## Background

The South Australian Cyber Security Framework (SACSF) and the South Australian Protective Security Framework (SAPSF) detail the importance of classifying information and associated information assets (such as ICT platforms and services) based on Confidentiality, Integrity and Availability requirements. Protection efforts should be prioritised for those assets and information that is considered critical to the ongoing operations of the agency. This guideline supports implementation of the SACSF Principle Two, *Information: Maintain the confidentiality, integrity and availability of all agency information and systems.*

The following documents should be read in conjunction with this guideline:

- South Australian Cyber Security Framework describes the requirements and expectations for agencies to protect information and information systems when stored digitally.
- South Australian Protective Security Framework[1] describes the South Australian classification scheme for confidentiality and provides translation from the earlier scheme used within government to the new markings.

## Guidance

This guideline outlines a process for classifying the integrity and availability of information and associated information assets. Details on identifying and classifying the confidentiality of these assets can be found within the SAPSF.

Identifying the integrity and availability levels of information assets assists an Agency to apply risk management techniques described in the SACSF across all ICT systems and organisational processes, allowing an agency to appropriately plan, resource and maintain effective information security controls.

## Characterising the value of information

The following tables describe the different Integrity and Availability classification levels. Using these descriptions, the information owner is able to classify the information to the appropriate level. The

[1] The SAPSF is still in development, however, the information security elements have been approved and released and will be referenced in this document. For further information about the SAPSF please contact: SAPSF@sa.gov.au

process recognises that information for the public may require exceptionally high degrees of integrity (accuracy) and availability.

## SOUTH AUSTRALIAN GOVERNMENT 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). |

## SOUTH AUSTRALIAN GOVERNMENT 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 |

## 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.

Information received by another entity, whether it is commercial or from government in other jurisdictions must not have its markings altered or changed without the express written consent of the originator of the information.

*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.*

## References, links and additional information

- South Australian Cyber Security Framework
- PC030 Protective Security Management Framework
- AS/NZS ISO/IEC 27002:2013
- NIST ID.AM
- Australian Government Protective Security Policy Framework

## Document Control

| | |
|---|---|
| ID | SACSF/G6.0 |
| Version | 1.0 |
| Classification/DLM | OFFICIAL |
| Compliance | Discretionary |
| Original authorisation date | November 2019 |
| Last approval date | November 2019 |
| Next review date | November 2020 |