South Australian Protective Security Framework

INFOSEC3:

Robust ICT and cyber security

SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK

Contents

Purpose

1. This policy describes how all South Australian Government agencies can safeguard their information and communication technology (ICT) systems to ensure the confidentiality, integrity and availability of official information. This includes defending against common and emerging cyber threats (e.g. bots, malware, ransomware, spam) and the threat of malicious insiders, while facilitating the continuous delivery of government business.

Core Requirement 9

Safeguard ICT systems from compromise to ensure confidentiality, integrity and availability of official information is maintained

Supporting Requirements

2. To safeguard ICT systems from compromise to ensure confidentiality, integrity and availability of official information is maintained, agencies[1] **must:**

   I. apply the appropriate processes and protections as outlined in the South Australian Cyber Security Framework (SACSF)

[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".

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.
SHOULD	Use of the word **should** (or **recommended**) indicates an action that agencies ought to undertake, unless prevented by legitimate circumstances or justification
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".
availability	allowing authorised persons to access information for authorised purposes at the time they need to do so
bot	an automated piece of software designed to perform a certain task, often imitating or replacing a real person's user behaviour
compromise	includes, but not limited to, loss, misuse, interference, unauthorised access, unauthorised modification, unauthorised disclosure.
confidentiality	limiting of access to information to authorised persons for approved purposes.
integrity	assurance that information has been created, amended or deleted only by the intended authorised means and is correct and valid
malicious insider	an employee, former employee, contractor or business associate with legitimate access to an agency system or data, who uses that access to steal or destroy data or sabotage systems. Knowledge of a malicious insider must be reported to the appropriate authorities
malware	malicious software
ransomware	a type of malware designed to deny access to a computer system or data until a ransom is paid
spam	an unsolicited or undesired electronic message

Acronyms

Acronym	Words
ASE	Agency Security Executive

SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK

Acronym	Words
ICT	Information and Communication Technology
ISMF	Information Security Management Framework
ITSA	Information Technology Security Adviser
SACSF	South Australian Cyber Security Framework

Guidance

South Australian Cyber Security Framework

3. The South Australian Cyber Security Framework (SACSF) has been developed to assist all agencies to identify and develop the cyber security requirements appropriate to their agency's function and risk profile. The SACSF replaces the former South Australian Information Security Management Framework (ISMF).

4. The SACSF provides considerable guidance for agency Information Technology Security Adviser's (ITSA) and security teams to assist with implementation within their agency.

5. Agencies **should** contact their ASE or ITSA for guidance on how the SACSF applies to their agency.

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, Intergovernmental and Diplomatic Relations	Date of approval: 25 November 2019
Revision number: 1.1	Date of review: 20 April 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	- Removal of word 'your' throughout entire document