South Australian Protective Security Framework

INFOSEC 3

ROBUST ICT AND CYBER SECURITY

Government
of South Australia

CONTENTS

POLICY

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

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 must:

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

GUIDANCE

SOUTH AUSTRALIAN CYBER SECURITY FRAMEWORK

3. The [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
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

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
2.0	14/11/2022	Policy reviewed, no changes