Government of South Australia

SACSF Ruling 7 – Maintaining supported IT products

SACSF/R7.0

Government Ruling on Cyber Security

Purpose

This Ruling provides a direction to South Australian (SA) Government agencies on the requirement to maintain supported information technology (IT) products.

Legacy systems present significant cyber security risk to government as they can increase the likelihood and impact of cyber security incidents due to the inability to patch security vulnerabilities.

Scope

The SA Cyber Security Framework (SACSF) applies to all SA Government public sector agencies, including administrative units, bodies corporate, statutory authorities, and instruments of the Crown as per the *Public Sector Act 2009*.

A SACSF Ruling is a mandatory application of a SACSF Policy Statement. This Ruling relates to the following SACSF Policy Statement:

> **2.7: Vulnerability Management**: Security vulnerabilities in agency ICT equipment, systems and applications must be identified and managed.

Ruling

SA Government agencies must ensure all IT products including software, hardware, firmware, systems, applications, and platforms, whether deployed on-premises, cloud-hosted, or in hybrid environments, are actively supported by the manufacturer, vendor or developer. This means:

- A contract with a manufacturer or vendor, or an appropriately skilled, dedicated internal resource, must be in place to ensure that IT products receive security updates as required[1], including critical vulnerability patches.
- The agency must have a clear lifecycle roadmap for IT products, including end of support dates and upgrade or replacement strategies.

Agencies must identify IT products approaching end-of-life (EOL) and:

- have a documented plan and roadmap to upgrade to a supported version prior to EOL, or
- have arrangements with a vendor to receive extended security updates, or
- have a plan to decommission the product prior to it becoming a legacy system.

Legacy systems are any IT product (i.e. hardware, software, services, protocols, and/or systems) that meet one or more criteria in **both** Category A and Category B below.

[1] For example, to align with an agency's defined patching timelines, when recommended by the vendor, or when advised to do so by the SA Government Watch Desk.

Category A:

- Out of support and extended support from the manufacturer, vendor or developer, or
- Considered an EOL product.

Category B:

- Impractical to update or support within the agency, or
- No longer cost effective, or
- Considered to be above the current acceptable risk threshold, or
- Offers diminishing business utility, or
- Prevents or obstructs fulfillment of the agency's IT strategies.

Where legacy systems cannot be immediately replaced, agencies must:

- Ensure that a legitimate business reason for maintaining the legacy system is documented and approved.
- Have a documented and approved plan in place, including timeframes, to replace or decommission the legacy system.
- Conduct a security risk assessment that is approved by the business owner of the system and the Agency Security Executive.
- Implement temporary mitigations as stated in Australian Signals Directorate's Managing the risks of legacy IT to bring the risk within the agency's risk appetite. For example:
  - Network isolation - Segregate legacy systems from sensitive networks to reduce exposure.
  - Access restrictions - Limit access to legacy systems to only essential personnel and enforce least privilege and multi-factor authentication.
  - Enhanced monitoring - Apply continuous logging and alerting to detect suspicious activity on legacy systems.
  - Implement attack surface reduction - Remove configuration weakness or minimise the capability and functionality of an application.
  - Schedule system availability and access - If only required for discrete periods, legacy systems should be shut down or closed when not in use to prevent unauthorised access.

Agencies must manage the risks arising from the vulnerabilities presented by legacy systems. The Agency Security Executive and agency IT Security Advisor must be consulted in the assessment and approval of a legitimate business reason for maintaining legacy systems.

Agencies must identify all legacy systems in their environment. The Department of Treasury and Finance (DTF) as the Control Agency for Cyber Crisis may require agencies to disclose legacy systems in their environment in response to a cyber security threat or incident in accordance with responsibilities under PC042 – Cyber Security Incident Management.

Exemptions

- Agencies that have assessed a legacy system as being high risk, and cannot apply the recommended temporary mitigations, must advise the Office of the Chief Information Officer by completing the exemption process.
- Exemptions must be sought through the Office of the Chief Information Officer exemption process.

Aboriginal Impact Statement

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

Roles and responsibilities

Position title or unit/team	Listed responsibilities
Chief Executive	Responsible for the effective implementation of, and compliance, with this Ruling within their agency.
Senior Executives, Directors and Managers	Responsible for ensuring • the Ruling is implemented and observed by staff • staff are fully informed of their obligations and responsibilities under the Ruling, and trained where required • any reporting requirements are met.
Agency Security Executives	Responsible for ensuring that the Ruling is implemented within the agency and that business processes support the Ruling requirements. Required to be consulted on and make informed, risk-based decisions on any requests for legitimate business use of legacy systems.
Agency IT Security Advisor	Responsible for providing advice on application of this Ruling within the agency environment, and for providing advice on the risks to agency information and services. Required to be consulted on and provide informed, risk-based advice on any requests for legitimate business use legacy systems.
All staff	Required to comply with this Ruling and any related procedures, and to play an active role in ensuring the compliance of others.

Related Documents

- South Australian Cyber Security Framework | Security SA
- South Australian Protective Security Framework | Security SA
- PC004-ICT-Digital-and-Cyber-Security-Requirements.pdf
- PC042-Cyber-Security-Incident-Management-V2.pdf
- ICT Policy Statement 1: Compliant Authorities
- Managing the risks of legacy IT: Practitioner guidance | Cyber.gov.au
- Patching applications and operating systems | Cyber.gov.au

Definitions

Relevant acronyms, words and terms in the standard and definition – delete if not required.

Term	Definition
Public Sector Agency	An internal to government entity, including administrative units, bodies corporate, statutory authorities, and instrumentalities of the Crown, as defined in the *Public Sector Act 2009* (SA).
End-of-Life	When a company ceases support for a product or service. This is typically applied to hardware and software products when a company releases a new version and ends support for certain previous versions.
Mitigation	A decision, action, or practice intended to reduce the level of risk associated with one or more threat events, threat scenarios, or vulnerabilities.
Legacy System	An information technology (IT) product (i.e. hardware, software, services, protocols, and/or systems) is considered legacy when it meets one or more criteria in both Category A and Category B below. Category A: • Considered an end-of-life product, or • Out of Support, and extended support from the manufacturer, vendor or developer. Category B: • Impractical to update or support within the entity, or • No longer cost-effective, or • Considered to be above the current acceptable risk threshold, or • Offers diminishing business utility, or • Prevents or obstructs fulfillment of the entity's IT strategies.
Patch	A piece of software designed to remedy vulnerabilities or improve the usability or performance of software, IT equipment or operational technology equipment.
Patching	The action of updating, fixing, or improving a computer program.
Vulnerability	A weakness in a system's security requirements, design, implementation or operation that could be accidentally triggered or intentionally exploited and result in a violation of the system's security policy.

Document Control

Approved by	CIO Steering Committee	Version	V1.0
Approved date	12 November 2025	Next review date	November 2027
Original date of approval	12 November 2025	Compliance	Mandatory
Contact	Cyber Security Directorate, Office of the Chief Information Officer		
Contact email	cybersecurity@sa.gov.au		