



SACSF/G11.0

GOVERNMENT GUIDELINE ON CYBER SECURITY

SACSF Guideline – Vulnerability management and patching

Purpose

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

This guideline has been developed to assist agencies and applicable suppliers to understand the vulnerability management and associated patching requirements of the SACSF.

Scope

This guideline applies to:

- SA Government public sector agencies (as defined in the [Public Sector Act 2009](#)), that is, administrative units, bodies corporate, statutory authorities and instrumentalities of the Crown.
- Suppliers to the SA Government and non-government personnel providing services to agencies.

The SACSF policy statement related to this guideline is:

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

Guideline

To meet SACSf requirements, agencies and associated suppliers are expected to implement and maintain vulnerability management and patching processes within their ICT environments.

Using vendor-supported applications and operating systems in agency workstations and servers, and patching associated security vulnerabilities in a timely manner, minimises the South Australian Government's exposure to risks associated with vulnerabilities in agency environments.

Security considerations	Mitigating controls
Identifying security vulnerabilities	Identify and track assets • The first step in accurately monitoring vulnerabilities is to know what information systems and assets exist within that environment. • To assist with this process, agencies should use existing asset registers where possible. Maintaining accurate asset registers helps agencies to understand where vulnerabilities may be putting their environments at risk of compromise. • It is recommended that the following information about each asset is included in the register: ○ Is the asset internal or external facing? ○ Does it support production, test, or development environments? ○ Who are the information owners? ○ Who are the system owners? ○ What business applications or processes does it support? ○ What is the impact of disruption or compromise? ○ What are the supporting operating systems and their patch level? • Asset registers should be available to the agency staff responsible for vulnerability management and patching processes. Identify vulnerabilities • Agencies may identify relevant security vulnerabilities using legitimate publications including: ○ Vulnerability databases such as the Common Vulnerabilities and Exposures (CVE) Program ○ SA Government-issued cyber security notifications, advisories and directives ○ Vendor notifications and bulletins ○ Industry advisories, alerts and vulnerability-reporting services such as the Australian Cyber Security Centre (ACSC) and the SA Government Cyber Security Watch Desk. • Security vulnerabilities may also be detected and identified through activities such as: ○ Cyber security risk assessments ○ Security event monitoring ○ Security incident investigations ○ Security metrics monitoring ○ Periodic vulnerability scanning

Security considerations	Mitigating controls
-------------------------	---------------------

- | | |
|--|--|
| | <ul style="list-style-type: none"> ○ Vulnerability assessments ○ Penetration testing, third-party audits or internal audits. |
|--|--|

Vulnerability scanning

- | | |
|--|---|
| | <ul style="list-style-type: none"> • Vulnerability scanning is typically an automated process using third party software tools to identify vulnerabilities and misconfigurations within an ICT environment. • These tools use a list of publicly known vulnerabilities to identify vulnerabilities in ICT equipment, systems and applications. They provide the agency with the broadest visibility of vulnerabilities and the greatest opportunity to mitigate associated security risks. • As a guide, agencies should aim to: <ul style="list-style-type: none"> ○ Use a vulnerability scanner with an up-to-date vulnerability database for vulnerability scanning activities ○ Scan at least daily to identify missing patches for security vulnerabilities in the operating systems of internet-facing services ○ Scan at least fortnightly to identify missing patches for vulnerabilities in the operating systems of workstations, servers and network devices ○ Scan at least fortnightly to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, software, and security products ○ Scan at least fortnightly to identify missing patches or updates for vulnerabilities in mobile applications (referred to as an app).¹ ○ Implement authenticated scanning to provide accurate insight by enabling the vulnerability scanner to identify vulnerabilities from a trusted viewpoint within the environment. <ul style="list-style-type: none"> ▪ use a dedicated scanning account that can be disabled between scans ▪ where possible, use public key authentication. ○ Define assets using the following tags, which make the scan results more readable and attributable: <ul style="list-style-type: none"> ▪ internal or external ▪ physical location ▪ asset owner ▪ operating system. ○ Assess and mitigate additional security risk introduced by unauthenticated and authenticated vulnerability scans. |
|--|---|

¹ These first four recommendations align with Maturity Level 1 in the [ACSC Essential Eight Maturity Model](#).

Security considerations	Mitigating controls
	○ All agencies conducting any penetration testing or vulnerability scanning on their applications hosted within StateNet or in the public cloud environment must notify WatchDesk and OCIO Network Security Governance team (grc@sa.gov.au) in advance. This is not necessary for applications hosted in public cloud environment, if the scanning is not going to interface with StateNet infrastructure. Penetration testing • Penetration testing is an assessment method that simulates an attack on a system to identify vulnerabilities. It tests existing security controls and helps agencies to gain an understanding of how significant the impact of a cyber-attack would be on data and business processes. • To maintain the confidentiality, integrity and availability of data, agencies should take a risk-based approach to penetration testing. As a guide, consider penetration testing: ○ At least once per year, both internally and externally, on systems that manage critical services or process sensitive data, particularly if those systems are internet-facing. ○ Immediately after completing a significant upgrade to ICT infrastructure, or systems that manage critical services or process sensitive data, particularly if those systems are internet-facing. ○ On any new system before being deployed. • Agencies should ensure that testing is conducted by independent and suitably skilled personnel for this purpose. • Prior to any testing being undertaken, an agreement and risk management plan should be implemented between agency and vendor which clearly defines the roles and responsibilities. Careful planning minimises the potential impact on the confidentiality, integrity or availability of the target system. • All agencies must notify the Watch Desk prior to conducting penetration testing. Agencies within StateNet must also notify the Across Government Service Desk. The notification must include details of the system being tested, dates, times and contact details for the vendor conducting the testing. Notification ensures the testing is not detected and mistaken for malicious activity.
Assessing security vulnerabilities	• Once vulnerabilities are identified, it is important for the agency to assess and prioritise the security vulnerabilities. • Standards such as the Common Vulnerability Scoring System (CVSS) indicate the potential impact of security vulnerabilities if exploited. Agencies should analyse identified security vulnerabilities based on the potential impact and likelihood of exploitation, in line with their existing risk management framework. • When prioritising the remediation of vulnerabilities, agencies should consider: ○ Does the vulnerability exist on critical systems?

Security considerations Mitigating controls

- What is the classification of information on the affected systems?
 - Is the affected system public facing?
 - Are there any existing mitigations that would limit the potential impact of exploitation?
 - Can a network or host-based IDS/IDP detect or prevent the vulnerability?
 - Could the agency respond quickly to an exploitation with the existing logging and alerts in place?
 - The higher the CVSS rating, the higher priority it should be to correct.
- Security vulnerabilities assessed as 'extreme' risk to the agency should be addressed first, within 48 hours according to the SACSf. An 'extreme' risk security vulnerability is defined as follows:
 - the security vulnerability facilitates remote code execution,
 - critical business systems are affected,
 - an exploit exists in the public domain and is being actively used, and/or
 - the system is internet-connected with no mitigating controls in place.

Mitigating security vulnerabilities

Where possible, agencies should utilise existing risk management frameworks for mitigation of exposure to security vulnerability risks or refer to *SACSf Guideline 8.0 Risk Management*.

Appropriate and timely mitigations or treatments based on effectiveness, cost and existing security controls should be taken in response to the level of risk to the agency's information assets.

Applying patches

- Regularly patching applications and operating systems in agency workstations and servers removes or reduces the likelihood of malicious actors exploiting known security vulnerabilities.
- Agencies should use a documented, managed approach to ensure that patches are applied consistently across their environment, including:
 - Obtaining patches from a known, trusted source
 - Verifying the integrity and authenticity of patches
 - Testing patches outside of the production environment to ensure patches work as expected
 - Implementing patches to production systems in a timely manner based on the context of the agency's environment
 - Following agency change management processes
 - Confirming that patches have been applied successfully.
- Where resources are limited, the deployment of patches can be prioritised to:
 1. Public/internet-facing services
 2. Important network devices, servers and workstations of high-risk users, which includes senior managers and their staff, system administrators, and staff working in human resources, finance and payroll
 3. All other network devices, servers and workstations.

Security considerations Mitigating controls

- Once a patch is released by a vendor, it should be applied in a timeframe that is commensurate with the risk posed to the agency. The SACSf recommends the following timeframes:
 - Tier One agencies: Patches for operating systems and applications for all workstations and servers are applied within one month of release, or within 48 hours for vulnerabilities assessed as 'extreme'.
 - Tier Two agencies: Patches for operating systems and applications for all workstations and servers are applied within two weeks of release, or within 48 hours if assessed as 'extreme'.
- The Australian Cyber Security Centre (ACSC) recommends these additional timeframes:
 - Patches for vulnerabilities in operating systems of IT equipment other than workstations, servers and network devices are applied within one month of release, or within 48 hours if an exploit exists.
 - Patches for drivers and firmware are applied within one month of release, or within 48 hours if an exploit exists.
 - Patches for internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists.
 - Patches for office productivity suites, web browsers and their extensions, email clients, software, and security products are applied within two weeks of release, or within 48 hours if an exploit exists.
- Other patches released to provide additional functionality or improvements may be installed at the discretion of the agency's asset owners and in accordance with existing change management processes.
- The decision not to apply patches should be recorded, appropriately risk-managed and accepted by the risk owner. Include a timeframe for reviewing the associated risk assessment.
- Further guidance on patch implementation can be accessed via the [ACSC Essential Eight](#) and [NIST Guide to Enterprise Patch Management Technologies](#).

When patches are not available

- In some cases, vulnerabilities cannot be mitigated by a patch, patches may not exist, or a patch could introduce unacceptable additional risk. Temporary workarounds and mitigation advice from vendors, trusted authorities or security researchers may provide some protection if no patches or updates are available for security vulnerabilities.
- When a vendor patch is not available, the decision as to whether a temporary workaround is implemented should be risk-based, as with patching. Temporary workarounds may include:
 - Disabling or blocking access to vulnerable functionality
 - Preventing exploitation of a security vulnerability
 - Containing the exploitation of a security vulnerability

Security considerations Mitigating controls

- Detecting attempted or successful exploitation of the security vulnerability.

Unsupported applications and operating systems

- Applications and operating systems that are no longer supported by vendors expose the agency to security vulnerabilities. Unsupported software and operating system versions should be removed, updated to a supported version, or replaced with alternative supported software.
- Where unsupported applications and operating systems are required for a specific purpose, the agency should manage the security risks and consider additional controls such as:
 - Implementing application control
 - Strengthening access controls such as MFA
 - Additional logging and monitoring
 - Isolating unsupported systems from the rest of the agency's environment
 - Limiting or adapting access, such as by privileged users, or to and from the internet.

Preparing for faults

- While it is rare that the deployment of a patch can lead to an application or operating system failure, the possibility should be considered when developing the agency's patch management processes. The risk of an outage occurring during the process, however, is far outweighed by the benefit of the additional security provided by patching the vulnerability.
- Prior to deployment, it is recommended that agencies test patches in a staging environment, roll the patch out to a small environment first, or deploy the patch widely and implement a rollback mechanism to a known good state if there is an issue.

Reporting vulnerabilities and patching compliance

- Agencies should use a mechanism to provide visibility on the vulnerability and the patch status of the agency's environment to ensure that known security patches and fixes have been implemented. Periodic scanning for known vulnerabilities and appropriate patch implementation should be conducted across all the agency's ICT equipment, systems and applications to identify patching compliance rates. Additional automated tools and utilities from reputable and trusted sources may assist in generating patching compliance reports and dashboards.
- Expected patching rates should be documented, and compliance or non-compliance reported on appropriately within the agency.
- Reports on trends in security vulnerabilities, risk, and patching also support the agency's cyber security assurance activities and reporting requirements, including security metrics.

Related documents

- [South Australian Cyber Security Framework \(SACSF\)](#)
- [Australian Government Information Security Manual \(ISM\)](#)
- [NIST Vulnerability Database](#) – Common Vulnerabilities and Exposures (CVE) Program, Common Vulnerabilities Scoring System (CVSS)
- [NIST Cyber Security Framework](#)
- [Australian Cyber Security Centre \(ACSC\) Essential Eight](#)

This guideline does not aim to provide the reader with all of the responsibilities and obligations associated with vulnerability management and patching. The individual requirements of agencies will have direct bearing on what measures are implemented to mitigate identified risk(s).

Definitions

Term	Definition
Security vulnerabilities	a flaw or weakness in an application or operating system that could be exploited by a threat.
Patching	applying software code updates to fix security vulnerabilities or other issues in an application or operating system.

DOCUMENT CONTROL

Approved by: CIO Steering Committee

Contact: Cyber Security

Email: cybersecurity@sa.gov.au

Division: Office of the Chief Information Officer

Compliance: Discretionary

Review number: V1.1

Original authorisation date: January 2023

Next review date: July 2026

Last approval date: 22 October 2024

Licence



With the exception of the Government of South Australia brand, logos and any images, this work is licensed under a [Creative Commons Attribution \(CC BY\) 4.0 Licence](#). To attribute this material, cite Department of Treasury and Finance, Government of South Australia, 2024.