SACSF/G12.0

GOVERNMENT GUIDELINE ON CYBER SECURITY

SACSF Guideline 12.0 - Vulnerability Disclosure Program Implementation Guideline

Purpose

This guideline defines how South Australian (SA) Government agencies can implement the requirements of the SA Government Vulnerability Disclosure Program.

Background

Security vulnerabilities in software and IT systems are discovered regularly. These vulnerabilities can be used by criminals and malicious groups to disrupt digital services and steal sensitive information.

The SA Government maintains a Vulnerability Disclosure Program to encourage and support individuals to identify and report security vulnerabilities that they find on government digital services such as websites.

Scope

This guideline applies to:

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

The SACSF Secure Web Service Standard statements related to this guideline are:

- **SACSF/S4.16 Secure Web Service Standard: Baseline Security Control 7 Vulnerability Disclosure Program** – All newly commissioned web services must maintain processes to manage the identification and reporting of vulnerabilities in alignment with the SA Government Vulnerability Disclosure Program Policy.

Scope inclusions

This guideline applies to all public-facing web services hosted either on SA Government network infrastructure, by third-parties, or cloud service providers (e.g. Amazon Web Services, Azure, Google) that are designed to be accessed and used by the public from the internet.

This includes all SA Government websites and associated systems such as:

- Web applications that are developed or modified by agencies and/or third parties.
- Commercial-off-the-shelf (COTS) software and mobile applications.
- System components such as internet login portals, web servers, external application programming interfaces (APIs), and public facing modules.

Scope exclusions

This guideline does not apply to:

- Web services that do not allow access from public networks.
- Internal web services hosted on the internal or external cloud infrastructure which only allow access from SA Government networks and accounts.

Guideline detail

The SA Government encourages individuals, including security researchers and security professionals, to identify and report security vulnerabilities on government digital services including websites, applications and supporting ICT infrastructure.

The SA Government maintains a Vulnerability Disclosure Program to manage the reporting and resulting vulnerability assessment and mitigation.

SA Government agencies must participate in the Vulnerability Disclosure Program by:

- Including a security.txt file in all newly commissioned web services.
- Including a link to the SA Government Vulnerability Disclosure Policy in the security.txt file.
- Maintaining a contact point, for example a shared mailbox or online form, for individuals conducting testing to report security vulnerabilities.
- Maintaining documented vulnerability management processes, including procedures for:
    - Assessing and verifying the risk from the vulnerability.
    - Prioritising activities to mitigate the vulnerability based on risk.
    - Communicating the vulnerability to relevant third parties.
    - Mitigating the vulnerability.
    - Ensuring all information received and created with respect to the vulnerability is handled in a confidential and secure manner.
- Prioritising the assessment and mitigation of vulnerabilities reported as part of the Vulnerability Disclosure Program.

- Maintaining a process for communicating with reporting individuals, which includes:
    - Acknowledging receipt of reported vulnerabilities.
    - If able to, advising the reporting individual of steps being taken to remediate the vulnerability.
    - Advising the reporting individual once the vulnerability has been mitigated.

The SA Government does not offer a monetary reward for the discovery and reporting of security vulnerabilities.

Agencies should consider including existing web services in the Vulnerability Disclosure Program.

Digital Signature

It is recommended that the security.txt file described in the next section be digitally signed using an OpenPGP cleartext signature. When digital signatures are used, it is also recommended that the "Canonical" field be used in the security.txt file, allowing the digital signature to authenticate the location of the file.

When it comes to verifying the key used to generate the signature, it is always the security researcher's responsibility to make sure the key being used is one they trust.

Implementing the security.txt file

The following are recommended steps to implement security.txt:

- Create the .txt file with the required fields (see next page).
- Create a folder on the web server called ".well-known" in which the security.txt file will be placed. This may require assistance from an external provider.
- Each subdomain requires its own security.txt file as there is no inheritance.
- Track the expiration date of the file and refresh when required.

```
Contact: mailto:example@sa.gov.au
Expires: 2023-12-30T22:30:00.000Z
Policy: https://example.com/disclosure-policy.thml
```

Screenshot of security.txt file text.

The file on the web service will contain the following fields:

Field Name	Required	Description	Example
Contact	Mandatory	A method that researchers should use for reporting security vulnerabilities such as a shared mailbox, a phone number, and/or a web page with contact information. List in order of preference.	Contact: mailto:*securitymailbox*@sa.gov.au Contact: tel: +61 8 1111 1111 Contact: https://example.com/security-contact.html
Expires	Mandatory	The date and time when the content of the security.txt file will expire. Update this value periodically.	Expires: 2023-06-30T09:00:00.000Z
Policy	Mandatory	A link to the SA Government Vulnerability Disclosure Policy, to help security researchers understand the SA Government's vulnerability reporting practices.	Policy: https://www.security.sa.gov.au/cyber-security/report-a-security-vulnerability
Encryption	Optional	A link to a key that security researchers should use for encrypted communication.	Encryption: https://example.com/pgp-ley.txt
Acknowledgements	Optional	A link to a page where security researchers are recognised for their reports and collaboration to remediate vulnerabilities.	Acknowledgements: https://example.com/hall-of-fame.html
Preferred-Languages	Optional	The set of natural languages that are preferred when submitting security reports.	Preferred-Languages: en, es, fr
Canonical	Optional	Link to the security.txt file to enable digital signing.	Canonical: https://www.example.com/.well-known/security.txt

Field Name	Required	Description	Example
		It is recommended that a “security.txt” file be digitally signed using an OpenPGP cleartext signature.	
Hiring	Optional	A link to any security-related job vacancies.	Hiring: https://example.com/jobs.html

Aboriginal Impact Statement

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

Reporting

Not applicable.

Related documents

- South Australian Government Protective Security Framework (SAPSF)
- South Australian Government Cyber Security Framework (SACSF)
- SA Government Vulnerability Disclosure Policy
- SACSF G11.0 Guideline – Vulnerability management and patching

Definitions

Term	Definition
SA Government 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)*.
Security vulnerability	A weakness in system security requirements, design, implementation or operation that could be exploited.
Web service	A service used to communicate between two devices on a network – e.g. web server, website, web application.
Web server	The infrastructure where a web site or web application runs. It may be dedicated hardware or virtualised and includes software components such as the operating system. It may be hosted on-premise, on third party infrastructure, or on cloud infrastructure (e.g. AWS or Azure).
Website	A collection of web pages and related content that is identified by a common domain name and published on at least one web server.
Web application	Application software which runs on a web server and is accessed using a web browser or software. Web applications are generally interactive and may connect to a backend database or another application server.

DOCUMENT CONTROL

Approved by: Chief Information Officer Steering Committee	
Contact: Chief Information Security Officer	Email: cybersecurityOCIO@sa.gov.au
Division: Office of the Chief Information Officer	Compliance: Mandatory
Version: V1.0	Date of last approval: 13 December 2023
Next review date: December 2024	Date of original approval: 13 December 2023