Government of South Australia

Vulnerability Disclosure Policy

DTF/P18.0

Across Government Policy

Purpose

This policy provides clear guidelines for individuals on how to identify and report security vulnerabilities as part of the South Australian (SA) Government Vulnerability Disclosure Program.

Policy detail

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

We maintain a Vulnerability Disclosure Program to manage vulnerability reporting and resulting assessment and mitigation.

Guidelines for individuals conducting testing:

- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Only use exploits to the extent necessary to confirm a vulnerability's presence. Do not use an exploit to compromise or exfiltrate data, establish persistent command line access, or use the exploit to pivot to other systems.
- Comply with all applicable state and federal laws.
- Once you have established that a vulnerability exists or encounter any sensitive data (including personal information, financial information, or other confidential information), you must stop your assessment, notify us immediately, and not disclose this data to anyone else.
- **The following test methods are NOT PERMITTED:**
  - Network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data
  - Physical testing (e.g. office access, open doors, tailgating)
  - Social engineering (e.g. phishing, vishing)
  - Clickjacking
  - Attempts to modify or destroy data
  - Testing third-party websites, applications or services that integrate with government services

- Any other non-technical vulnerability testing.

How to report a vulnerability:

- Report all security vulnerabilities that you discover in a timely manner.
- Submit the report through the address listed under Contact in the **security.txt** file associated with the digital service that the vulnerability was discovered on to report the vulnerability.
- If there is no security.txt file, report it to watchdesk@sa.gov.au.
- Give as much information as possible, including details of the potential security vulnerability, the services it affects, and steps to reproduce the vulnerability including any proof-of-concept code if applicable.
- When you report a vulnerability, please keep it confidential and provide us with a reasonable amount of time to fix or mitigate it.

What government will do when we receive your report:

- We will work with you to understand and resolve identified vulnerabilities quickly.
- Vulnerabilities will be managed in accordance with internal vulnerability management procedures which may include:
  - Assessing and verifying the risk from the vulnerability.
  - Prioritising activities to mitigate the vulnerability based on risk.
  - Mitigating the vulnerability.
  - Communicating the vulnerability to relevant third parties.
  - Ensuring all information received and created with respect to the vulnerability is handled in a confidential and secure manner.

How government will work with you:

- We will promptly respond to any reports received and to the best of our ability advise you of remediation steps being undertaken.
- If further information is needed by us to verify the vulnerability, we may contact you again.
- We will advise you when the vulnerability has been rectified.
- No monetary reward is offered by government for the discovery and reporting of security vulnerabilities.

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 relevant.

Definitions

Term	Definition
Security vulnerability	A weakness in system security requirements, design, implementation or operation that could be exploited.

Related Documents

- South Australian Protective Security Framework (SAPSF)
- South Australian Cyber Security Framework (SACSF)
- SACSF Guideline 11.0 Vulnerability Management and Patching
- SACSF Guideline 12.0 Vulnerability Disclosure Program Implementation

Document Control

Approved by	CIO Steering Committee	Version	1.1
Approved date	25 November 2025	Next review date	November 2027
Original date of approval	September 2023	Compliance	Mandatory
Contact	Office of the Chief Information Officer, Cyber Security Directorate		
Contact email	cybersecurity@sa.gov.au		