Department of
Creative Industries, Tourism and Sport

CITS Vulnerability Disclosure Policy

ARTS AND CULTURE TRUST

AGWA

STATE LIBRARY WESTERN AUSTRALIA

WAM WESTERN AUSTRALIAN MUSEUM

Contents

1 Purpose

The purpose of this policy is to establish clear guidelines for cyber security researchers engaging in vulnerability discovery activities related to the Department of Creative Industries, Tourism and Sport (CITS) and the Cultural Statutory Authorities (CSAs) systems and outlines expectations for responsible disclosure.

By defining the scope of acceptable cyber security research, submission procedures, and our response practices, this policy aims to foster collaboration while ensuring the security of our digital assets.

2 Scope

This policy applies to:

- Cyber security researchers (ethical hackers).
- Internal stakeholders, such as CITS Cyber Security Team.
- External vendors such as software providers, security consultants or auditors.

This policy applies to systems and services owned and operated by CITS and the CSAs, including:

- CITS
- Office of Multi-cultural Interests
- Tourism WA
- State Records Office
- WA Museum
- State Library of WA
- The Arts and Culture Trust
- The Art Gallery of WA

A security.txt file will be published on all CITS and CSA websites and web applications, providing contact information for reporting potential vulnerabilities.

Out of Scope:

Specific systems and services that are out of scope:

- The Arts and Culture Trust website (www.artsculturetrust.wa.gov.au)
- The Art Gallery of WA (AGWA) website (www.artgallery.wa.gov.au)

Systems listed above, including any third-party services or integrations, are excluded from scope, and not authorised for testing. If you aren't sure whether a system is in scope, please contact CITS Cyber Security at vulnerability.disclosure@cits.wa.gov.au to discuss.

Websites hosted on other wa.gov.au subdomains are not in scope and not authorised for testing under the CITS Vulnerability Disclosure Policy.

The following activities are out of scope and not permitted against any system:

- Denial of service (DoS/DDoS) and spam
- Social engineering (e.g. phishing) against CITS staff
- Physical access attacks (e.g. attempting to access buildings).
- Uploading malware, backdoors, webshells, or other "weaponised" exploits that could degrade system security or affect other users.

- Attempts to access or manipulate accounts that do not belong to you (e.g. resetting passwords for other users).
- Attempts to modify or destroy data.

In general, low severity issues without a direct security impact (weak SSL cipher suites, missing HTTP security headers, SPF/DKIM/DMARC misconfiguration, etc) will not be considered in scope.

3 Definition of terms

Cultural Statutory Authority (CSA): Means the Art Gallery of Western Australia, Arts and Culture Trust, State Library of Western Australia, and Western Australian Museum.

Cyber Security Researcher: Individuals who are external to and not otherwise contracted by CITS and the CSAs (commonly referred to as ethical hackers), who identify, analyse, and report potential security vulnerabilities in systems, applications, or infrastructure. These individuals provide such information to the department through responsible disclosure practices outlined in this policy.

External Vendors: Third-party organisations or service providers that supply products, services, or support to your agency but are not part of your internal structure. In the context of vulnerability reporting and ICT risk, they may include:

- Software providers
- Cloud service providers
- Managed service providers (MSPs) services.
- Hardware vendors
- Security consultants or auditors
- Telecommunications providers
- Third-party integrators

Policy: A statement of the mandatory principles guiding an organisation's operations and significant decision-making.

Vulnerability: A flaw in code or design that creates a potential point of security compromise for an endpoint or network. Vulnerabilities create possible attack vectors, through which an intruder could run code or access a target system's memory.

Western Australian (WA) Government Cyber Security Policy: A formal directive that outlines the minimum cybersecurity requirements for all WA public sector agencies to protect government systems, data, and services from cyber threats.

4 Policy and Guideline

This policy enables cyber security researchers to identify and report vulnerabilities on in scope systems.

Internal stakeholders who identify a vulnerability should refer to the Information and Security Management Policy for the internal vulnerability disclosure policy statement.

This policy is in addition to, and does not replace or override, any vendor or platform terms, acceptable use requirements or security testing policies that apply to CITS systems (for example Azure and Microsoft 365). You must comply with both this policy and any applicable vendor requirements. If there is a conflict, the more restrictive requirement applies.

4.1 How to report a vulnerability

To report a vulnerability, please submit all reports to vulnerability.disclosure@cits.wa.gov.au

To expedite the triaging and prioritisation of submission, your reports should:

- Describe where the vulnerability was discovered and the potential impact of exploitation.
- Include enough detail so we can reproduce your steps. Screenshots and proof of concept code are helpful.

4.2 What happens next

The Cyber Security team will coordinate with you as openly and as quickly as possible during the remediation of any identified vulnerabilities.

We will:

- Notify you within 5 business days that we have responded to your report.
- Keep you informed throughout the internal investigation and remediation (if required) of the identified vulnerability.
- Agree on a date for public disclosure.
- Credit you as the person who discovered the vulnerability unless you prefer to remain anonymous. CITS does not offer financial compensation for reported vulnerabilities.

5 Related guidance

This policy is in alignment, and should be read in conjunction with the WA Cyber Security Policy

6 Document information

The policy will be reviewed at minimum every two years.

Approved by:	Corporate Executive	Date: 8/04/2026
For:	The Department of Creative Industries, Tourism and Sport	
Endorsed by:	Chief Executive Officer	Date: 17/04/2026
For:	State Library of Western Australia	
Endorsed by:	Director	Date: 29/04/2026
For:	Art Gallery of Western Australia	
Endorsed by:	Director Strategy and Governance	Date: 30/04/2026
For:	Western Australian Museum	
Endorsed by:	Chief Executive Officer	Date: 4/05/2026
For:	Arts and Culture Trust	
Status	Approved	
Version	1.0	
Policy Owner	Director ICT Operations and Cyber Security	

Primary Contact	Manager Cyber Security
Effective date	8/04/2026
Next review date	8/04/2028
File reference	E26045739

6.1 Revisions

Version	Date	Reviewer	Details of revision
1.0	11/03/2026	Leon Koh, Senior ICT Risk and Policy Officer	Creation of this policy document

6.2 Version history

Version	Date	Name & Position / Committee	Status / Notes
1.0	26/03/2026	Corporate Policy Committee	Approved
1.0	8/04/2026	Corporate Executive	Approved
1.0	8/04/2026	Director General	Approved