Government of **Western Australia**
Department of **Training**
and Workforce Development

CYBER DISCLOSURE POLICY

EFFECTIVE: 23 MAY 2024

VERSION: 1.0

DOCUMENT MANAGEMENT

Equity impact assessment

This policy considers and reflects where appropriate the principles of the Department's:	
☐ Disability access and inclusion plan	☐ Language services policy
☐ Workforce diversity and inclusion policy	☐ Innovate reconciliation action plan
☐ Substantive equality policy	☐ Employment policy
☒ Not applicable	

Approval

(To be completed by the Office of the Director General)

Corporate Executive endorsement date	23.05.2024
Director General approval to publish date	04.07.2024
Policy reference number	2024-05

Version control

(To be completed by the Office of the Director General)

Version	Date	CM reference	Brief description
1.0	04.07.2024	TWD/D24/0113694	New policy

CONTENTS

1. POLICY STATEMENT 4
2. SCOPE 4
3. PRINCIPLES 5
4. BACKGROUND 5
5. DEFINITIONS AND ACRONYMS 5
6. PROCEDURES 6
7. GUIDELINES 7
8. RELATED POLICIES AND OTHER RELEVANT DOCUMENTS 7
9. RELEVANT LEGISLATION 7
10. REVIEW DATE 7
11. CONTACT INFORMATION 7

1. POLICY STATEMENT

The Department is committed to ensuring the security of the people of Western Australia by protecting their information. This policy provides guidelines for security researchers on how to report vulnerabilities and what to expect in return from the Department.

This policy describes what systems and types of research are covered under this policy, how to send us vulnerability reports, and what can be expected from us.

This policy addresses the WA Government's Cyber Security requirement section 1.7 Vulnerability Disclosure Program - each entity must implement a vulnerability disclosure program.

2. SCOPE

In scope
This policy applies to the following internet-accessible systems and services:
dtwd.wa.gov.au
Jobs and Skills Centres | Jobs and Skills WA
Welcome! | Migration WA
Muresk Home (dtwd.wa.gov.au)
WA State Training Board (stb.wa.gov.au)
www.tafeinternational.wa.edu.au
TAMS Portal (dtwd.wa.gov.au)
Training Accreditation Council (www.wa.gov.au)

Out of scope
Any service not listed above (e.g. connected services) are excluded from scope and not authorised for testing. Additionally, vulnerabilities found in any third-party services or systems should be reported directly to the vendor. If you aren't sure whether a system is in scope or not, contact us at securitynotifications@dtwd.wa.gov.au before starting your research (or at the security contact for the system's domain name listed in the .gov WHOIS).

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

- Denial of service (DoS/DDoS) tests or other tests that impair access to or damage a system or data;
- Social engineering (e.g. phishing, vishing);
- Physical access attacks (e.g. attempting to access buildings, open doors, tailgating);
- Spam;
- Uploading malware, backdoors, webshells, or other "weaponized" 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);
- Any attempts to modify or destroy data;
- Any other non-technical vulnerability testing; and
- Any low severity issues without a direct security impact (weak SSL cipher suites, missing HTTP security headers, SPF/DKIM/DMARC misconfiguration).

3. PRINCIPLES

The Department encourages researchers to report potential vulnerabilities.

If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorised. We will work with you to understand and resolve the issue quickly, and the Department will not recommend or pursue legal action related to your research. Should legal action be initiated by a third party against you for activities that were conducted in accordance with this policy, we will make this authorisation known.

As a public entity, the Department cannot offer compensation for discovered vulnerabilities. We will instead, with your consent, publish researcher names and give credit for discovering vulnerabilities under the “people who have disclosed a vulnerability to us” banner.

4. BACKGROUND

The Department has implemented a cyber disclosure program to align with the WA Government Cyber Security Policy. Implementing a cyber disclosure program assists agencies by improving the security of their applications and systems.

The Department’s cyber disclosure program is a collection of processes and procedures designed to identify, verify, resolve, and report on vulnerabilities disclosed by people who may be internal or external to organisation.

The development, implementation and maintenance of a cyber disclosure program will improve the Department’s cyber security posture and assist in risk mitigation. The Cyber Disclosure Policy is a key component of the program.

5. DEFINITIONS AND ACRONYMS

Vulnerability
A flaw in code or design that creates an adverse reaction in an application or computer system and can lead to compromise or shutdown of an endpoint or network as well as exfiltration of data or information.

Vulnerability Disclosure
The practice and process of reporting vulnerabilities to the appropriate parties.

SSL cipher suites
Sets of instructions on how to secure a network through Secure Sockets Layer (SSL).

Sender Policy Framework (SPF)
An email authentication method that helps to identify the mail servers that are allowed to send email for a given domain.

Hypertext Transfer Protocol (HTTP) security headers
Directives used by web applications to configure security defences in web browsers.

DomainKeys Identified Mail (DKIM)
A protocol that allows an organisation to take responsibility for transmitting a message by signing it in a way that mailbox providers can verify. DKIM record verification is made possible through cryptographic authentication.

Domain-based Message Authentication, Reporting and Conformance (DMARC)
A standard that prevents spammers from using your domain to send email without your permission - also known as spoofing.

6. PROCEDURES

How to report a vulnerability
To report a vulnerability, please submit through our HTTPS (secure) web form or email securitynotifications@dtwd.wa.gov.au Reports may be submitted anonymously.
Note: We do not support PGP-encrypted emails.

What we would like to see from you
To help us triage and prioritise submissions we recommend that your reports:

- describe where the vulnerability was discovered and the potential impact of exploitation;
- offer a detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts or screenshots are helpful); and
- be in English, if possible.

What you can expect from us
If you share your contact information with us we will:

- acknowledge receipt of your report within five business days;
- keep you informed throughout our internal investigation and remediation (if required) of the identified vulnerability;
- maintain an open dialogue to discuss issues;
- agree on a date for public disclosure; and
- credit you as the person who discovered the vulnerability unless you prefer to remain anonymous.

Information submitted under this policy will be used for defensive purposes only - to mitigate or remediate vulnerabilities. If your findings include newly discovered vulnerabilities that affect all users of a product or service and not solely this Department, we may share your report with the Australian Cyber Security Centre. We will not share your name or contact information without express permission.

Questions regarding this policy may be sent to securitynotifications@dtwd.wa.gov.au
We also invite you to contact us with suggestions for improving this policy.

7. GUIDELINES

Under this policy, “research” means activities in which you:

- notify us as soon as possible after you discover a real or potential security issue;
- 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;
- provide us a reasonable amount of time to resolve the issue before you disclose it publicly; and
- do not submit a high volume of low-quality reports.

Once you’ve established that a vulnerability exists or encounter any sensitive data (including personally identifiable information, financial information, or proprietary information or trade secrets of any party), **you must stop your test, notify us immediately, and not disclose this data to anyone else**.

8. RELATED POLICIES AND OTHER RELEVANT DOCUMENTS

- WA Government Cyber Security Policy

9. RELEVANT LEGISLATION

- Western Australian Criminal Code 1994 section 440a

10. REVIEW DATE

23 May 2026

11. CONTACT INFORMATION

ICT
Corporate