# Vulnerability disclosure policy

This policy aims to safeguard the people of Western Australia by securing their information, and it provides guidelines for security researchers on how to report vulnerabilities and what to expect in return from the Department of Water and Environmental Regulation.

## About this policy

We are committed to ensuring the security of the Western Australian public by protecting your information. This policy is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and to convey our preference in how to submit any discovered vulnerabilities.

This policy describes the systems and types of research covered under this policy, how to send us vulnerability reports, and what you can expect from us.

If you make a good faith effort to comply with this policy during your security research, we will not take any legal action against you.

We will not compensate you for finding potential or confirmed vulnerabilities.

## What this policy covers

### In scope

This policy applies to the following systems and services:

- Water website and its subdomains (water.wa.gov.au)
- Environmental website (der.wa.gov.au)
- Department of Water and Environment Regulation subdomains only (for example cps.dwer.wa.gov.au, consult.dwer.wa.gov.au)
- Keep Australia Beautiful Council WA website (www.kabc.wa.gov.au)
- Environmental Protection Authority website and its subdomains (www.epa.wa.gov.au)
- Offsets register website (www.offsetsregister.wa.gov.au)
- Waste Authority website (www.wasteauthority.wa.gov.au)
- Office of the Appeals Convenor (www.appealsconvenor.wa.gov.au)

### Out of scope

Systems not 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 us at vulnerability@dwer.wa.gov.au.

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 department staff
- physical access attacks (e.g. attempting to access buildings)
- upload of 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)
- any 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.

## How to report a vulnerability

To report a vulnerability, please submit all reports via email to vulnerability@dwer.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.

## What happens next

We will coordinate with you as openly and as quickly as possible during the remediation of any identified vulnerabilities.

We will:

- respond to your report within five (5) business days
- keep you informed throughout the department’s 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.

## People who have disclosed vulnerabilities to us

Below are the names or aliases of people who have identified and disclosed vulnerabilities to us: