# Vulnerability disclosure policy

## About this policy

The security of our systems and the data we hold is a priority for MEGT. We make every effort to keep our ICT systems secure. Despite our efforts, there may still be vulnerabilities.

This policy allows a person, for example a security researcher, to share their findings with us in good faith. If you think you have found a potential vulnerability in one of our ICT systems, products and/or services, please tell us as quickly as possible.

MEGT will not generally compensate you for finding potential or confirmed vulnerabilities. However, in certain circumstances we may consider offering compensation.

This policy covers any ICT systems, products and/or services operated by, or on behalf of, MEGT.

This policy does not cover the following activities, which MEGT considers to be malicious:

- Clickjacking
- Social engineering or phishing
- Denial of service (DoS or DDoS) attacks
- Posting, transmitting, uploading, linking to, or sending malware
- Physical attacks
- Deliberate attempts to access, modify or delete sensitive data

## How to report a vulnerability

To report a vulnerability please email **InformationSecurity@megt.com.au.** Please include enough detail so that MEGT can reproduce your approach.

Any vulnerability reported under this policy, and any data accessed or obtained, must be kept confidential, except to the extent that disclosure is required by applicable law. Do not make details of any vulnerability and/or data public.

MEGT reserves the right to take legal action if the existence of a vulnerability, or data obtained, becomes public knowledge through your act or omission in breach of this policy.

## What happens next

MEGT will:

- Respond to your report within five (5) business days
- Keep you informed of the progress of our investigation and resolution

If MEGT decides to disclose the vulnerability then, with your consent, we will credit you with the discovery.

# People who have disclosed vulnerabilities to us

Below are disclosed vulnerabilities, a name is included if consent has been given by the person(s) who identified it:

No vulnerabilities recorded at this time