Privacy Commissioner
Te Mana Matapono Matatapu

Vulnerability Disclosure Policy

If you find a security issue with our online systems, please tell us so that we can get it fixed. Our goal is to protect people's privacy. That means getting vulnerabilities fixed as soon as possible. It also means encouraging people to tell us about vulnerabilities. So we want to work with anyone who tells us about vulnerabilities in our system.

As far as practicable we use components of the New Zealand Government Common Web Platform (CWP). [See: https://www.cwp.govt.nz/]. If the vulnerability is in a CWP component then we will need to pass the information on to the Department of Internal Affairs. But we will not pass on your contact details without your permission. DIA do not have a vulnerability disclosure policy.

1. How to tell us

Email us at security@privacy.org.nz. If you want to encrypt your email our public key is available from: https://privacy.org.nz/assets/Complaints/PGP-Public-Key.txt.

2. What to tell us

Please tell us what you can of the following information without doing any further work on the vulnerability.

- Type of vulnerability
- Whether the vulnerability has been published or shared with others
- Affected products and versions
- Affected configurations
- Step-by-step instructions / proof of concept codes to replicate the issue
- Was personal information exposed?
- What has happened with any personal information exposed.

3. What we will do

We acknowledge receipt as soon as possible and within 7 working days we will give you an update on the progress of our investigation.

We will look at the reported vulnerability and work with the appropriate service provider to validate the reported vulnerability. We will notify you of what that investigation found and what we decided to do.

We aim to address all vulnerabilities as quickly as possible but are reliant upon contracted suppliers.

If appropriate we will also handle this as a privacy breach and tell people whose personal information may have been disclosed. You can read about how data-related privacy breaches are handled in our "Data Safety Toolkit:. https://privacy.org.nz/news-and-publications/guidance-resources/data-safety-toolkit/.

We will work with you if you want to publicly disclose finding the vulnerability.

4. What you should not do

Some types of behaviour are not reasonable research approaches. Please do not try actions that can cause harm.

- "Denial of Service" (DoS) attacks
- Accessing data or information that does not belong to you. Once you see there is a problem that exposes information, please do not look for more such information – one example is enough
- Destroying or corrupting data or information that does not belong to you
- Sharing any personal information you obtained.

5. Protecting other people's privacy

Please do not share with others any vulnerability that you find until we have had the opportunity to fix the vulnerability. We don't want others trying to exploit the vulnerability.

Please do not share any personal information obtained from the Office, because that could cause harm to others. Posting personal information could constitute a breach of the Privacy Act which we might then have to investigate.

6. Our commitment

If you act in good faith and follow this policy, then we make the following commitments to you:

- The information that you share with us as part of this process will be kept confidential within OPC and our directly contracted suppliers
- Your contact details will not be shared with third parties, eg. DIA for Common Web Platform vulnerabilities, without your permission
- We will not initiate legal action against people attempting to find vulnerabilities within our systems who adhere to this policy

- If you report a vulnerability that materially affects our services or infrastructure, we will publicly acknowledge your help.

Contact details

If you have any queries, contact the Office of the Privacy Commissioner:

Call free on 0800 803 909 or

Email security@privacy.org.nz

www.privacy.org.nz