# Responsible Disclosure Policy

| Date | Version # | Change Description |
|---|---|---|
| 21/11/2025 | 1.0 | Published |

At Aussie Broadband, the security and privacy of our customers and systems is a top priority. We know that ethical security researchers, customers, partners, and the broader cyber security community play a vital role in helping us identify and fix vulnerabilities before they can be exploited.

That's why we've created this Responsible Disclosure Policy; to outline how we work with security researchers and what we expect from those who want to help us improve our security.

## Who this policy is for

This policy is designed for:

- Ethical security researchers and penetration testers not already engaged under contract with ABB
- Cyber security professionals
- Customers or users who discover vulnerabilities*
- Technical partners or vendors

If you fall into one of these groups and think you've found a security issue, we want to hear from you.

## What you can test

You can conduct responsible security research on Aussie Broadband systems, products, and services that are:

- Public-facing and internet-accessible
- Within your authorised access level (e.g., customer or user portal access)

**Not sure if something is in scope? Reach out to us first through the web form.**

## Rules of Engagement

We ask that you follow these rules when conducting research:

- Act in good faith and avoid causing harm or disruption
- Only test systems you're authorised to access
- Never access, modify, store, or exfiltrate customer or system data
- Avoid denial-of-service attacks or anything that degrades service
- Comply with all applicable laws
- Report vulnerabilities to us as soon as reasonably possible



* Excluding ABB staff

Aussie Broadband

## What's Not Allowed

Some activities are strictly off-limits:

- Social engineering, phishing, or impersonation
- DoS or DDoS attacks
- Physical attacks on property or personnel
- Clickjacking
- Data modification or destruction
- Accessing accounts or data that aren't yours
- Uploading or linking to malware
- Sending spam or unauthorised communications
- Testing third-party systems
- Using deceptive techniques to bypass security
- Any activity that violates the law

## Out-of-Scope Vulnerabilities

We appreciate all reports, but please do not report security vulnerabilities relating to missing security controls or protections that are not directly exploitable. Examples include:

- Weak or misconfigured SSL/TLS certificates
- Misconfigured DNS records (SPF, DKIM, DMARC)
- Missing HTTP security headers
- Theoretical CSRF or cross-site framing attacks
- Automated scan results without manual validation
- Vulnerabilities without a working exploit
- MITM or physical access-based attacks
- Issues requiring excessive user interaction
- Content spoofing without HTML/CSS impact
- CSRF on non-sensitive pages
- Public files with no sensitive content
- Non-sensitive cookie flags
- Vulnerable libraries without exploit paths
- Issues affecting outdated browsers
- Static resources in public buckets
- Verbose error messages or software version disclosures
- Rate limiting issues on non-auth endpoints
- Open redirects without security impact
- CSV injection without exploit

## How to Report a Vulnerability

If you believe you've found a security issue, fill out the web form with as much detail as possible, such as:

- Description of the vulnerability.
- Affected URLs, services, or assets.
- Steps to reproduce
- Proof-of-concept code or screenshots.
- Test accounts or objects used.
- Your contact details (optional).

We also ask that you:

- Submit reports in English
- Keep your findings confidential until we've resolved the issue
- Avoid exploiting the vulnerability
- Submit one vulnerability per report (unless chaining is necessary)

We won't share your contact details without your permission unless required by law.

**Please note:** We won't respond to messages unrelated to security vulnerabilities.

## What Happens After You Report

Once you submit a report, we'll acknowledge it within 48 hours. We may reach out for more information and will keep you updated on our progress.

## Safe Harbour

We appreciate your efforts and want to protect researchers acting in good faith. We won't take legal action if:

- You follow this policy
- You avoid unauthorised access
- You act in good faith
- You stop testing once a vulnerability is confirmed
- You cooperate with us on coordinated disclosure

If you're unsure whether your actions are covered, contact us first.

## Compensation

We don't offer monetary rewards or compensation for vulnerability disclosures. Your submissions are voluntary and help us strengthen our security for everyone.

---

**Thank you for helping us protect our customers and systems.**

**If you believe you've found a security issue, please let us know by filling out the vulnerability disclosure web form with as much detail as possible.**

**aussiebroadband.com.au**

* Excluding ABB staff

Aussie Broadband