nbn Vulnerability Disclosure Policy

Unclassified | S0066-240526625-67 | Rev 2 | 30 JUN 21
Owner: Darren Kane, Chief Security Officer

Purpose

The security of **nbn**'s networks and facilities is our top priority and we take every care to provide a trusted and secure network for all Australians.

As part of this commitment**, nbn** appreciates the importance of working with the security community.

This policy provides guidelines for security researchers to directly submit details of suspected security vulnerabilities in **nbn**'s Network and Facilities.

Policy

If you report a vulnerability to **nbn** under this Policy, we ask that you keep your submission confidential while we work with you to investigate the situation and beyond, to maintain the confidentiality of information within.

Always exercise caution and restraint when analysing and reporting suspected vulnerabilities and comply with this Policy. This includes taking extreme care when handling personal information, and not knowingly engaging in any activity that causes nuisance to any other users or person including by way of attacks against third parties, social engineering, denial-of-service attacks, or spam.

Accessing or attempting to access, modify, copy, exfiltrate or destroy any data is strictly prohibited under this Policy.

This Policy does not cover or permit any abuse, interference with or malicious acts towards any **nbn**™ Network, System or Facility that has the effect of, either directly or indirectly:

- causing performance degradation or impacting any **nbn**™ service in any way.
- impacting the availability or integrity of **nbn**'s Networks and Systems and **nbn**™ Facilities.
- compromising the confidentiality of communications carried on or contained in **nbn**'s Networks and Systems and **nbn**™ Facilities.
- otherwise causing any disruption to or interference with **nbn**'s Networks and Systems and **nbn**™ Facilities.

We are unable compensate you for finding potential or confirmed vulnerabilities.

How to report a vulnerability

To report a vulnerability, please send an email to: **VulnerabilityDisclosure@nbnco.com.au**

Please help us by providing as much information as you can so we can verify the suspected vulnerability, including the following:

- Your name and contact details.
- Description of the suspected vulnerability.

- Discovery date.
- List of the affected Networks, Systems or Facilities.
- Steps required for **nbn** to reproduce the suspected vulnerability.
- Other relevant details to allow **nbn** to verify and reproduce the suspected vulnerability.

What happens next?

We will (as appropriate):

- Acknowledge the receipt of your report within 5 business days using the contact information supplies above.
- Treat your report confidentially and not share any of your information unless required to do so to comply with **nbn**'s legal obligations.
- Keep you informed of our progress.
- Work with you regarding issues of attribution and/or public disclosure.

nbn is collecting your personal information to help you with your enquiry. **nbn**'s Privacy Policy sets out how we handle personal information, how you may access, or correct your information, how to make a complaint about **nbn**'s handling of your personal information and how we will deal with your complaint. If you have any questions or concerns about your privacy or personal information that **nbn** may hold, you can contact us by calling 1800 687 626 or emailing privacyofficer@nbnco.com.au. **nbn** uses service providers to carry out our work. Some of our service providers are located outside Australia.