Responsible disclosure policy

Data security is a top priority for nPlan, and nPlan believes that working with skilled security researchers can identify weaknesses in any technology.

If you believe you've found a security vulnerability in nPlan's service, please notify us. We will work with you to resolve the issue promptly.

Disclosure Policy

- If you believe you've discovered a potential vulnerability, please let us know by emailing us at support@nplan.io. We will acknowledge your email within 24 hours.
- Provide us with a reasonable amount of time to resolve the issue before disclosing it to the public or a third party. We aim to resolve critical issues within 24 hours of disclosure.
- Make a good faith effort to avoid violating privacy, destroying data, or interrupting or degrading the nPlan service. Please only interact with accounts you own or for which you have explicit permission from the account holder.

Exclusions

While researching, we'd like you to refrain from:

- Spamming
- Social engineering or phishing of nPlan employees or contractors
- Any attacks against nPlan's physical property or data centers

Thank you for helping to keep nPlan and our users safe!

Changes

We may revise these guidelines from time to time. The most current version of the guidelines will be available on our website.

Last updated: 1 Nov 2021