The ultimate guide To VDP: How to write a vulnerability disclosure policy

BY ANNA HAMMOND · APRIL 14, 2021 · LAST UPDATED ON NOVEMBER 17, 2025

If you're thinking about inviting ethical hackers to work with you, you're in the right place. This article will help you maximise the success of using ethical hackers by asking them to follow a vulnerability disclosure process. Before we explain how to write a vulnerability disclosure policy (VDP) let's start by covering some of the basics.

What is a vulnerability disclosure policy?

A vulnerability disclosure policy (VDP) provides ethical hackers with an outline for submitting vulnerabilities to an organisation. As well as mitigating the risk of security issues going undetected, having a VDP helps businesses to:

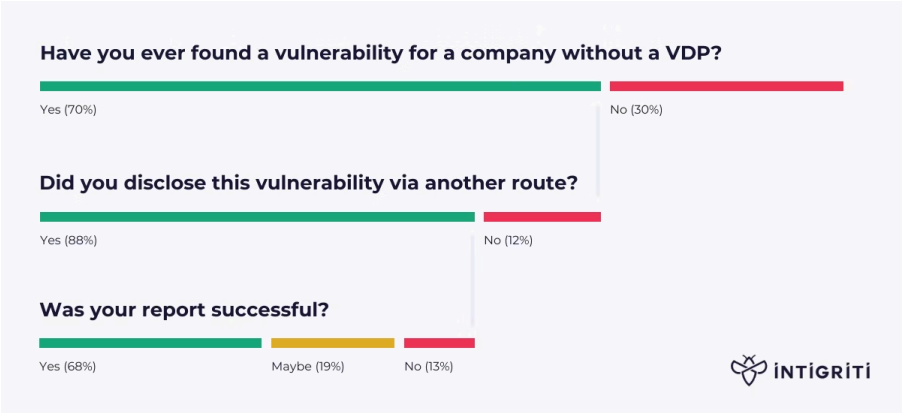
- Streamline their vulnerability reporting process
- Show a commitment to information security and data protection
- Build trust among stakeholders and customers
- Establish a set of rules for hackers to follow when testing your service.

A disclosure policy applies to any researcher reporting a vulnerability. However, it's also an opportunity for organisations to demonstrate their willingness to work with external actors working in good faith.

Why do you need a vulnerability disclosure policy?

Not having a vulnerability disclosure policy in place can lead to conflict between what should be a successful collaboration between two parties. Alternatively, researchers may not report a bug if there is no viable way to do so.

For example, according to the Ethical Hacker Insights Report, within Intigriti's community, 70% of researchers say they've found a vulnerability for an organisation that doesn't have a VDP. Of that group, 12% didn't escalate the report. For those that did, 32% of them said they weren't sure whether the submission successfully passed through the disclosure process. Together, that's 44% of the risks that potentially remain undetected.



Source: [The Ethical Hacker Insights Report 2021](#) by Intigriti

Without being aware of potential security risks, you cannot fix them. For this reason, companies need a vulnerability disclosure policy if they want to invite ethical hackers to contribute to their security.

How to write a vulnerability disclosure policy

A VDP needs to include information about what the researcher and organisation can expect from the disclosure process. We suggest the below six key components:

1. Company background
2. Commitments
3. Scope
4. Legalities
5. Reporting methods
6. What to expect after a submission

Six components to include in a vulnerability disclosure policy

1. Company background

Make sure to provide a brief background on your business within this opening section. For example:

- Who you are
- Your business purpose
- Your speciality
- Customers
- Other relevant stakeholder groups.

The reason for providing context around your business is because it helps the researcher know what is important to you from a security standpoint.

2. Commitments

In this section, you can declare your commitments to customers and stakeholders, and explain how you intend to keep their data safe. This is a good opportunity to introduce why you have the policy, and how it helps your business honour its promises.

3. Scope

The scope is mostly directed at security researchers but is helpful for other stakeholders (such as partners, regulators and the media) to be aware of too. The essence of this section is to guide researchers on what is okay to test for vulnerabilities. However, the scope also highlights:

- Types of vulnerabilities that should be reported
- Products, features or assets that your company would especially like researchers to test
- Behaviour that is not allowed, such as disruption testing or privacy violations.

A good scope will not only clearly explain what the company perceives to be inside of the scope but also what they perceive to be on the outside. Doing this helps put everyone on the same page from the offset.

4. Legal safe harbour

You want them to disclose bugs in your system responsibly without being fearful of legal consequences. Therefore, it's important to give security researchers permission to act and assure that no legal action will be taken against them, provided they remain in scope.

You're actively trying to encourage ethical hackers to participate. Therefore, the language you use should be clear and concise but also inviting. Here is an example of what you could write as part of your safe harbour policy:

"[Your company name] considers ethical hacking research conducted consistent with this policy to constitute as "authorised" under criminal and civil law. [Your company name] will not pursue civil action or initiate a complaint about accidental, good faith violations.

If legal action is initiated by a third party against you and you have complied with the Terms, [Your company name] will take steps to make it known that your actions were conducted in compliance and with our approval."

5. Reporting methods

This section is about establishing the process for how ethical hackers should submit vulnerabilities to your business. Be as clear as possible and never assume contributors will know what information you need to process a report. Cover aspects such as:

- Preferred communication channels
- What information they should include
- Whether you want submissions written in a specific language.

Bear in mind that the researchers have already invested significant time and effort to test your systems so it's important to only ask for information you'll genuinely need. Ask for too much and you may put

contributors off entirely.

6. What to expect after a submission

This area of the policy is a good place to outline how reports will be evaluated and what happens if they're accepted or rejected. You should also define a timeline for when they can expect to hear from you.

Including this information helps to manage expectations with regards to what kind of acknowledgements, recognitions and remuneration researchers can expect to receive. You should also indicate when researchers will know (if at all) whether they can publicly disclose a vulnerability they reported to you.

Where should you publish your VDP?

Now that you understand how to write a vulnerability disclosure policy, you can decide whether it is best situated on your website or a bug bounty platform.

Hosting a VDP on your website

Some companies choose to add their VDP directly on their website. Having a specific page dedicated to contributors will allow them to get in touch and provide information the way you desire. Companies that opt for this disclosure path can go to securitytxt.org to add a security.txt file to their website, then follow their proposed steps forward.

Using a bug bounty platform to manage vulnerability disclosure

A bug bounty platform is what many companies use to publish their bug bounty program. Like a vulnerability disclosure policy, a program includes the six components mentioned above: company background, scope, commitments, reporting process, and what to expect after a submission. To see an example, Randstad provides a great vulnerability disclosure policy example included as part of their bug bounty program.

With a bug bounty platform, the vulnerability disclosure process is managed by a third party. This helps streamline the entire process, but it also taps into an already engaged community of ethical hackers who have experience in submitting reports.

Those that have less experience in vulnerability disclosure can lean on the support of a triage team. These experts work with researchers to ensure reports are valid, in-scope, and correctly submitted. For businesses, this helps reduce the likelihood of them receiving duplicate reports and ensures the information in submissions cover the vulnerability adequately.

Ready to streamline your vulnerability disclosure process? Speak to a member of the Intigriti team today to request a demo.

REQUEST A DEMO