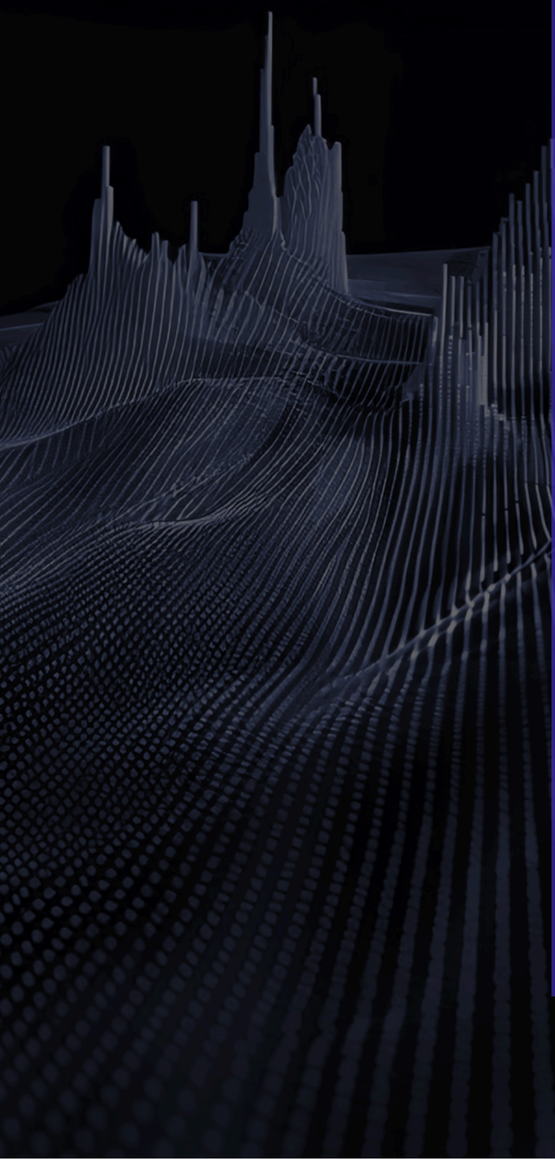
VDP Checklist: Critical Components and Best Practices for a Successful VDP

If your organization wants to know about potential security threats before they can be exploited, you must first open a channel for external entities to alert you of those risks. A vulnerability disclosure program (VDP) is a structured method for third parties and security researchers to report vulnerabilities responsibly before they can be exploited by malicious actors.

While every organization is different, there are several requirements for any VDP, as well as best practices that will further enhance the success of your program.



Requirements

□ **Promise Statement**
An organization's promise statement demonstrates to the public that it is proactive regarding vulnerabilities and takes threats seriously. Through an opening statement, organizations show customers and investors their good faith commitment to ongoing cybersecurity.

□ **Scope**
Scope specifies which assets and vulnerability types you'd like external parties to focus on, and which ones you'd like to exclude. Limitations may be established for products or versions, and to protect data or intellectual property.

□ **Safe Harbor**
Safe harbor fosters a secure and collaborative VDP by stating an organization's promise to protect those who disclose vulnerabilities from legal action. This section is essential for encouraging external parties to disclose bugs through an organization's official channel.

□ **Process Description**
The process description details the report submission and remediation process. Reports should include the severity of the vulnerability, how attackers could exploit it, and how developers can reproduce the bug. This information helps security teams prioritize threats and quickly validate new disclosures. A thorough process description can dramatically reduce time and minimize your exposure to attack.

□ **Preferences**
In your program preferences, you can set non-binding expectations for how reports will be evaluated. You should include expected response times, whether your organization will publicly disclose bugs, and whether the finder will receive confirmation upon repair. Regardless of how long a bug takes to fix, transparent communication between organizations and reporters builds trust and confidence within the VDP.

Best Practices

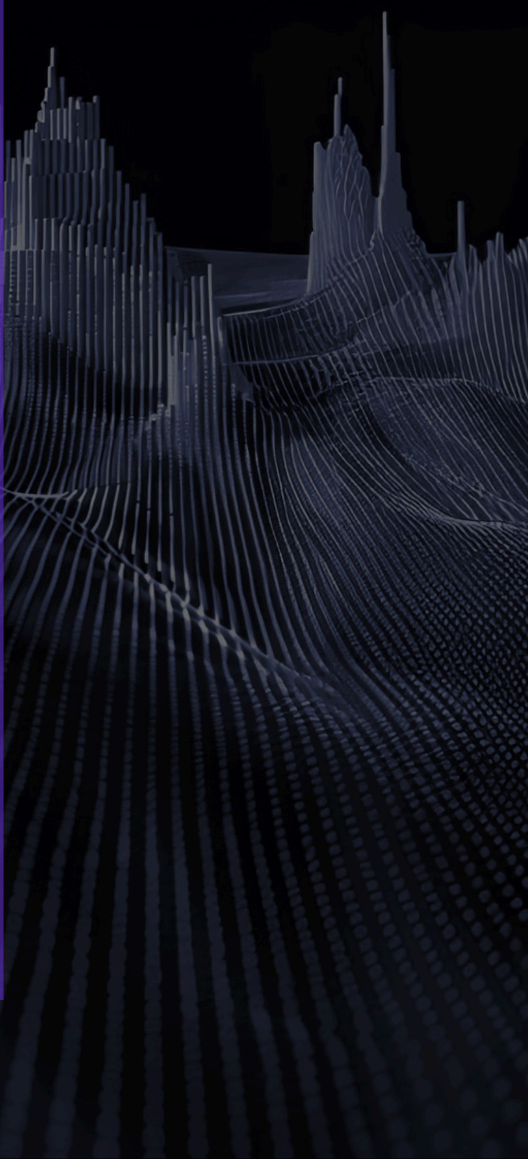
□ **Get Stakeholders Involved**
A VDP is most effective when it forms the foundation of a comprehensive program for vulnerability reporting, disclosure, triage, resolution, communication, and metrics. This means involving more than just the security team; engineering, legal, product, and compliance teams should also play a role. It's important to consider how incoming vulnerability reports will be routed into the appropriate systems, evaluated, and triaged by the right teams to ensure a coordinated and effective response. Make sure both internal and external stakeholders have clear information about the process, as well as a point of contact for any questions.

□ **Understand Your Compliance Requirements**
Compliance with laws, regulations, and industry standards is a key reason to implement a VDP. Understanding the specific requirements of frameworks like NIST, ISO, and country-specific laws such as the UK's PSTI is crucial. Aligning your VDP with these mandates helps you avoid penalties and ensures you can continue doing business with entities that require it.

□ **Dedicate Resources for Remediation**
Triage is essential for prioritizing vulnerability reports based on severity and potential impact. Efficient triage ensures that the most critical vulnerabilities are promptly addressed. If your organization lacks in-house triage capabilities, you may need to develop this internally or consider outsourcing to ensure timely and accurate handling of reports. As your VDP matures, robust triage processes will become increasingly vital.

□ **Determine the Right Level of Support**
Different organizations have varying needs when it comes to launching and managing a VDP. Determine whether your team will require ongoing support, such as assistance in communicating with external entities, or advisory services to keep your organization protected as you scale.

□ **Consider System Integrations**
Integration is critical to the success of your VDP. Your program should be fully integrated with existing systems, including legal, compliance, development, and security team workflows. All stakeholders must be involved and informed when vulnerabilities are reported. This coordinated approach prevents gaps in response and ensures that nothing falls through the cracks. Leveraging integrations also helps you embed findings directly into your SDLC.



Top Vulnerability Disclosure Programs

To see examples of high-performing programs,
take a look at some leading organizations' VDPs.

General Motors | Ohio Secretary of State | John Deere

> As we evolved our vulnerability management process, we realized a missing component was an easy way for an external security researcher to report an issue. HackerOne has helped fill that gap, helping us further mature our approach to vulnerability management.

James Johnson
CISO, John Deere

How to Get Started

With VDPs becoming an essential—and often mandated—part of security strategies, deploying one is more crucial than ever. Fortunately, solutions like HackerOne Response streamline the process, ensuring you can meet regulatory demands while protecting your organization.

We're here to help. HackerOne Response is the industry-standard VDP product trusted by The U.S. Department of Defense, Goldman Sachs, General Motors, Adobe, and many more to securely and seamlessly receive and act on discovered vulnerabilities. To learn more, visit hackerone.com.