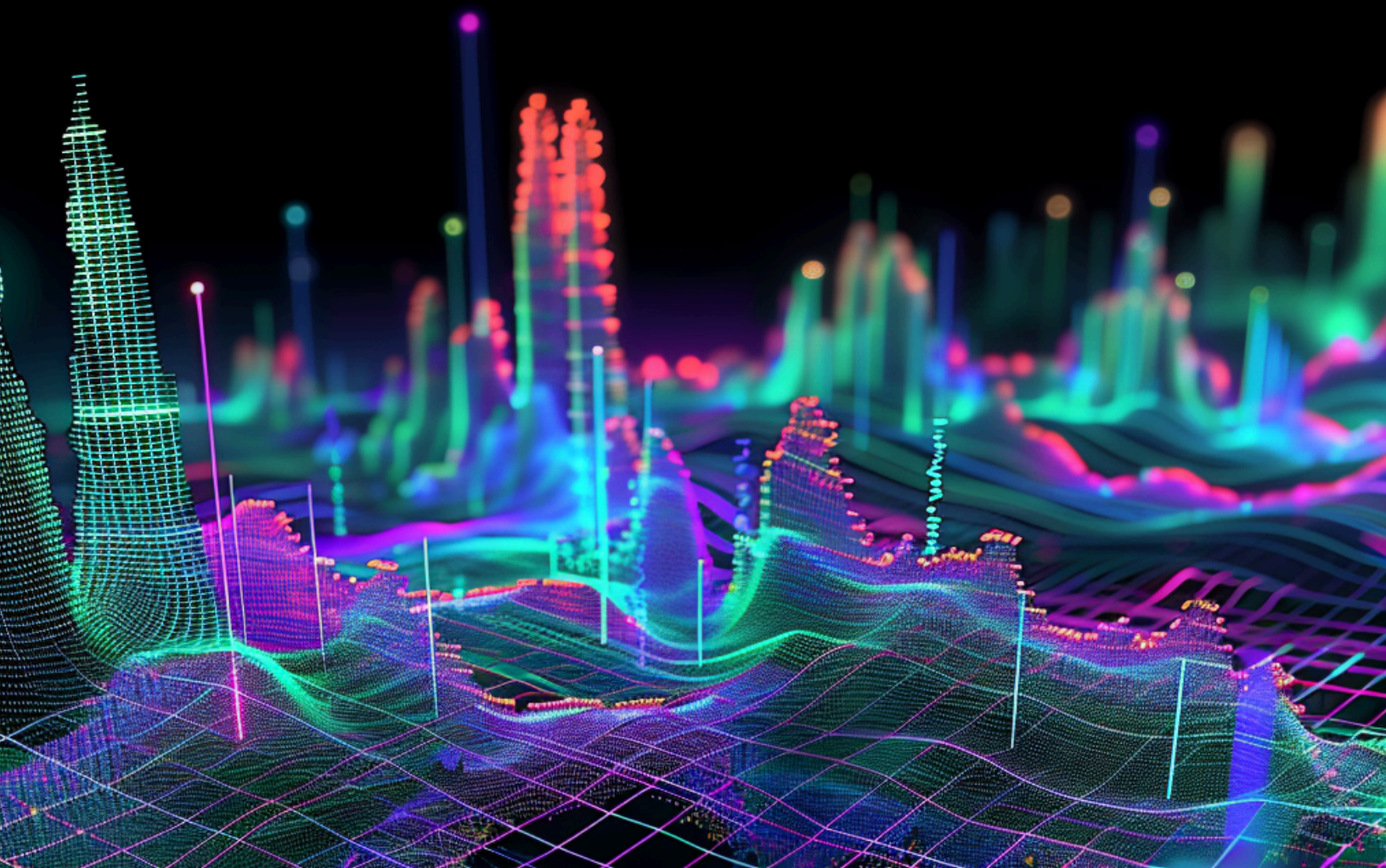
hackerone

Vulnerability Disclosure Programs (VDPs): A Comprehensive Guide

What a VDP Is, Why You Need One for Security and Compliance, and How to Get Started



Evolving from a security best practice to a compliance mandate, VDPs are table stakes in the mission to strengthen application and data security.

Your business thrives in the digital world, which comes with constant exposure to potential threats. The pressing question is: do you want to know about these threats before they are exploited?

Given the rise in data breaches and stricter compliance requirements, the answer should be a resounding yes. However, organizations must first open a channel for external entities to alert them to potential vulnerabilities.

A vulnerability disclosure program (VDP) is a solution recommended and used by organizations ranging from the U.S. Department of Justice and the U.K. Ministry of Defence to General Motors and Goldman Sachs. What's more, a VDP is increasingly included in regulatory mandates and compliance requirements.

Why are these organizations and so many regulatory agencies adamant about VDPs? Because they work to protect digital assets. For example, the U.S. Department of Defense alone has received over 50,000 vulnerabilities through its VDP—thousands of potentially exploitable vulnerabilities that would have gone unfixed without such a program.

So, what is a VDP, and how can you launch your own? Let's take a look.

Why Adopting a VDP Is a Security Best Practice

When a third party finds a vulnerability, they often try to inform your security team. But without a clear reporting channel, they face a tough choice: stay silent or go public. This can lead to vulnerabilities being either unreported or exposed on public channels, which can cause brand damage and draw attention to the issue before it can be addressed. Meanwhile, reports sent to a general email address can easily be overlooked, leaving serious vulnerabilities unresolved.

For these reasons and more, a VDP has become a universally recommended aspect of security. It establishes public-facing guidelines with a clear path for submitting vulnerabilities, fostering a proactive "see something, say something" culture. Serving as a digital neighborhood watch, a VDP helps you reduce the risk of security incidents and maintain control over the vulnerability management process. This layer of defense helps you meet compliance requirements, strengthen security, and address issues before they lead to real-world attacks.

To see an example, take a look at some leading organizations' VDPs here:

General Motors | **Ohio Secretary of State** | **John Deere**

> Implementing the VDP helped us triage and supplemented the internal team we were building. We also knew that the federal government was mandating VDP policies for their agencies, and we wanted to be on the forefront of embracing that security policy for our own constituents.

Jillian Burner
CISO, Ohio Secretary of State

5 Critical Components of a VDP

Every successful VDP includes five core components. Each plays a crucial role and protects the relationship between the finder and the business. Companies should lay out each component within disclosure guidelines displayed publicly as part of the VDP.

1. 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.

2. 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.

We strongly recommend incorporating all of your company's digital assets within the scope—however, there may be exceptions to consider. A limited scope risks leaving significant vulnerabilities unreported and unresolved.

3. 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.

4. 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 remediation time and minimize your exposure to attack.

5. 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.

Thriving in a New Era of Regulatory Compliance

Adopting a VDP is no longer just a best practice; it's increasingly encouraged and even mandated by legislation, regulations, and global compliance frameworks. Examples include:

- **Product Security and Telecommunications Infrastructure (PSTI) Act:** This U.K. law requires companies to provide publicly available information on how to report security issues and to publish at least one point of contact in English for security-related issues concerning their products (hardware or software). This includes setting clear expectations of when notifiers will receive acknowledgments and status updates in an accessible, clear, and transparent manner, without any prior request.

- **National Institute of Standards and Technology (NIST) SP 800-53 - Control RA-5(11):** This U.S. standard recommends software vendors establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.

- **ISO/IEC 27001:2022:** This widely used standard for information security management systems requires a public channel for reporting vulnerabilities (e.g., a VDP) and notes that bug bounty may help an organization meet some of the best practices.

Some laws and regulations, like PSTI, impose heavy fines for non-compliance, while others, particularly in the U.S., restrict organizations from doing business with entities like the federal government if they fail to comply.

As regulations and industry standards increasingly require organizations to have processes for receiving and handling vulnerability reports, a structured VDP becomes essential. It supports compliance efforts and can facilitate passing audits.

To help you understand which policies may impact your operations, we've developed an interactive Global Vulnerability Policy Map. **Explore our global vulnerability disclosure policy map.**

How to Get Required Attestation Documentation

On March 11, 2024, CISA and the Office of Management and Budget (OMB) released the Secure Software Development Attestation Form to help ensure that software providers to the federal government leverage minimum secure development techniques and toolsets. The new self-attestation requirements for providers of software to the U.S. government went into effect on June 11, 2024, for "critical software" and on September 11, 2024, for all other in-scope software.

These requirements include attesting to a public vulnerability disclosure process. Failure to provide the Attestation Form will prevent federal agencies from using or purchasing that software.

Who Are The People Reporting Vulnerabilities—and Why Trust Them?

For many organizations—particularly those bound by stringent compliance requirements or operating in highly regulated industries—working with third-party security researchers or "ethical hackers" sounds like a risk despite its proven benefits in reducing security threats.

Prospective customers often ask, "How can I trust researchers and hackers?" and "How do I maintain control of my environment?"

Here's the truth: bad actors are going to try to attack you, which is why it's crucial to have ethical experts on your side, who know how attackers think. When launching a HackerOne VDP, your program gains visibility among the world's most trusted and elite community of security reseachers.

Security researchers are motivated by more than money:

78%

say they do it to learn

47%

say they hack to protect and defend businesses and end users

(Source: 7th Hacker-Powered Security Report)

Meet the Researchers Behind the Report

Justin Gardner *(@Rhynorater)*

Justin is a full-time bug bounty hunter, having previously worked as a penetration tester and IT architect. Justin has competed in nearly every HackerOne Live Hacking Event and deep-dived many private/public HackerOne programs. As a result, he has found over 450 vulnerabilities and reached the top 35 in the HackerOne all-time leaderboard.

> At their core, many hackers are motivated by curiosity. Through working with HackerOne, organizations can harness and incentivize that curiosity to keep their customers safe from bad actors.
>
> **Rhynorater**

Jim Green *(@green-jam)*

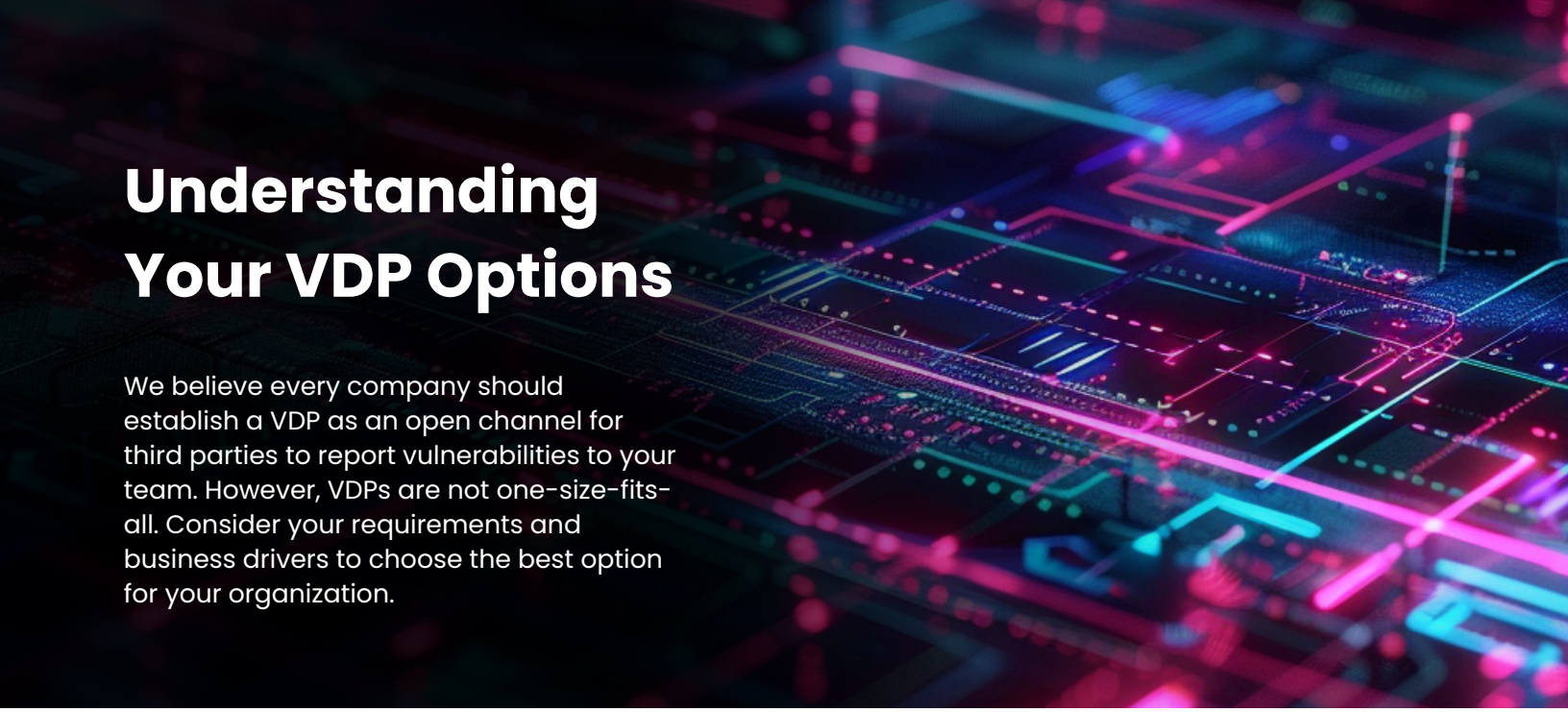
Jim is a solution architect working for a major bank and does security research in his spare time. Jim's experience in software development has allowed him to pick up a "sixth sense" for bad coding practices. Jim is the HackerOne Brand Ambassador for the U.K., promoting ethical hacking in the region and heading up the team for the Ambassador World Cup.

> "Hackers are like locksmiths rather than burglars. Software development and hacking are two halves of the same coin; as a solution architect with 20 years of experience in software development, I have reviewed a huge number of projects over the years with secure and insecure code. Like many other security researchers, I have picked up a bit of a 'sixth sense' for bad coding practices that helps me find bugs that other less experienced developers and security researchers may miss.
>
> **Green-jam**

Joseph Thacker *(@rez0)*

Joseph is a security researcher specializing in application security and AI. He has helped Fortune 500 companies find vulnerabilities that could have damaged brand trust or resulted in millions in legal action. With contributions to over 1,000 vulnerabilities ethical hacking platforms, Joseph is passionate about identifying issues through hacking, teaching, or consulting. His professional experience includes roles as a security analyst, engineer, and researcher. He holds a master of science in cybersecurity and information assurance, a bachelor of science in computer science, and certifications such as Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (C|EH), Computer Hacking Forensic Investigator (C|HFI), and CompTIA Security+.

> Ethical hackers are like the neighborhood watch. We're constantly on the lookout for potential threats and help keep everything safe. By trusting ethical hackers, companies stay one step ahead of bad actors and dramatically improve their security posture. We've got the same skills as malicious hackers, but we use them to find and fix vulnerabilities before the bad actors can exploit them.
>
> **@rez0**



Understanding Your VDP Options

We believe every company should establish a VDP as an open channel for third parties to report vulnerabilities to your team. However, VDPs are not one-size-fits-all. Consider your requirements and business drivers to choose the best option for your organization.

Not Recommended: Ad Hoc Reporting

Organizations may opt to use a security@myorganization.com email address as their VDP's reporting method, relying on a rotating team to check and triage incoming emails. Some organizations might even use a customer support solution to manage these reports, depending on the system and support staff to correctly route and track security-related messages.

However, these manual, ad hoc approaches are ineffective at best and dangerous at worst. You risk losing track of critical vulnerabilities, which could mean the difference between proactively resolving an issue and protecting your brand, customers, and data, or facing a security breach with its associated fallout and penalties. Fortunately, there is a better way.

Compliance Driven

For smaller companies with a limited number of annual external vulnerability reports, a free, self-serve VDP is a great option. Rather than struggling with an internally managed program, a VDP can deliver a consolidated view of all disclosed vulnerability reports. HackerOne Response Essential VDP is a free VDP offering that helps you align with industry standards —including self-serve onboarding, best-practice disclosure guideline templates, and the ability to integrate an @security email or embedded submission form into one inbox for centralized reporting with CVSS severity ratings, plus support from Hai, an AI copilot, to support prioritization and deliver faster remediation timelines.
Learn more here.

Security Driven

Midsize companies often require a more robust VDP with advanced features and support. Due to an increasing number of vulnerability reports, they often benefit from enhanced tools to streamline communication with hackers, along with reporting and analytics to identify trends and take proactive measures. At this level, they may also want the ability to select triage services to efficiently evaluate and prioritize each incoming report and determine remediation steps.

HackerOne Response Professional VDP is ideal for companies that require:

- Detailed reporting and analytics within the HackerOne Platform, along with tools to streamline communication with external entities.
- A vulnerability disclosure page hosted by HackerOne, with the ability to list on the HackerOne directory for increased visibility among our trusted community of security reseachers.
- Integration with security tools and development workflows for smoother collaboration.
- Ability to add on triage services to help you evaluate and prioritize each incoming report with remediation guidance.

Brand Driven

Enterprises with stringent security and compliance requirements—especially those with complex, multi-region operations—demand comprehensive and customizable VDPs. With high stakes, stakeholders and C-suite executives are fully invested in understanding the critical importance of a robust program.

To ensure ongoing security and compliance, CISOs prioritize advanced integrations for seamless collaboration across departments, complete triage services, and dedicated support to safeguard the organization at every level.

HackerOne Response Enterprise VDP is ideal for companies that require:

- Ability to centralize complex vulnerability-management activities within a single interface, optimizing operational oversight for more efficient security management.
- Extensive integration capabilities, with premium integrations and custom SLAs to meet specific compliance requirements.
- World-class triage services to handle comprehensive vulnerability assessment, including analysis, validation, reproduction, deduplication, prioritization, enrichment, and contextualization, ensuring you receive actionable insights to resolve issues quickly.
- Dedicated account management and 24x7 priority support for personalized guidance, plus tailored resources to enhance the success and growth of your program.

Who Relies on HackerOne

Customers from a variety of industries and across the globe rely on HackerOne Response.

TOYOTA · Goldman Sachs · GM · JOHN DEERE

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

"It is critical that organizations have a way for external parties to tell them about potential security vulnerabilities, leveraging their internal vulnerability management process to triage and remediate them."

Jason Pubal
Director of Perimeter Security, Financial Services Company

Beiersdorf

"Our Web Development Team has a tough job, and they do it very well. As an additional layer of defense, we decided to use the global knowledge of ethical hackers via a VDP, so we could be informed even when it is actually too late (meaning a vulnerability is published) but still early enough to identify and remediate the vulnerability before a malicious actor might find it."

Kai Widua
CISO, Beiersdorf

More Best Practices for VDP Success

Along with incorporating the five critical components of a VDP discussed earlier, consider the following best practices when developing a VDP that supports your security and compliance goals.

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.

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 U.K.'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.

hackerone

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**