hackerone

Vulnerability Disclosure Policy:

What Is It, Why You Need One, and How To Get Started

Recommended by industry and government leaders, VDPs are table stakes in the effort to increase application and data security.

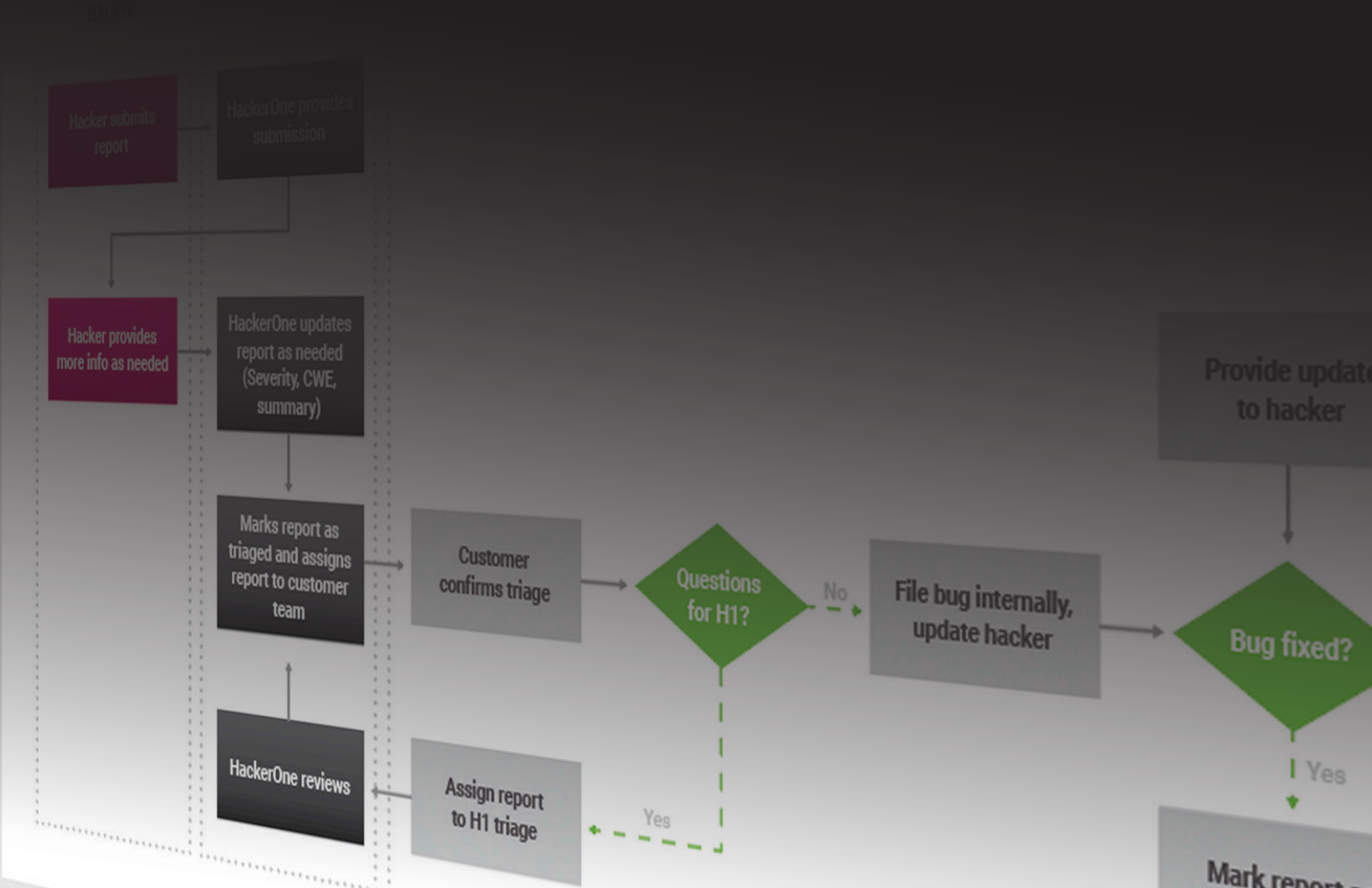


Table of Contents

Bug bounty programs may capture the majority of headlines in hacker-powered security today, but organizations must first open a channel for ethical hackers to alert them to potential vulnerabilities. It's called a vulnerability disclosure policy (VDP), and it's promoted extensively by voices as diverse as the U.S. Department of Justice to the European Commission to General Motors.

Why are these organizations so adamant about VDPs? Because they work and they protect assets. For example, the Department of Defense alone has received over 5,000 valid vulnerabilities through their VDP. That's thousands of potentially exploitable vulnerabilities that would have gone unfixed had they not been reported. It's no wonder they want everyone else to have one, too.

So what is a vulnerability disclosure policy and how can you launch your own? Let's take a look.

What is a Vulnerability Disclosure Policy?

A VDP is the digital equivalent of "if you see something, say something." It's intended to give ethical hackers (also known as "researchers" or "finders"), or anyone who stumbles across something amiss—clear guidelines for reporting potentially unknown or harmful security vulnerabilities to the proper person or team responsible.

Think of this real-life analogy: you walk past a neighbor's house and see their back door was left wide open. What would you do? You'd probably knock on their door, holler to see if they were home, or maybe even call them.

But for technology, it's not that simple. You might not know how to contact them, where to find a phone number or email address. Furthermore, you wouldn't know if your email or voicemail ever made it to the correct person, or anyone at all. Or, after looking for and not finding an appropriate contact channel, most of us would probably just give up.

The result, nearly every time, is that nothing happens...except that the vulnerability remains and the organization is unaware.

Understandably, a finder can become frustrated with the lack of a clear vulnerability reporting channel and *publicly* disclose it in an uncoordinated fashion. Maybe they tag your organization on social media, alerting potentially tens of thousands of individuals to your security gap. It happens in an instant, long before you have time to investigate or even begin working on a fix.

VDPs give finders clear directions on how to report a potential vulnerability, **They eliminate the potential business chaos should someone not know how to report a vulnerability and it winds up on social media.**

Darran Lee Hamer
@DarranHamer
Follc

@Cisco @CiscoSecurity tried to report possible security vulnerability with SPA phones. Told to buy a service contract to so. Unbelievable

Santhosh Tuppad
@santhoshst
Follow

Hey @CocaCola Does this website coke2home.com belong to you? I wanted to report a security vulnerability. #ResponsibleDisclosure

April C. Wright
@aprilwright
Follow

@CapitalOne How can I report a security vulnerability related to your website?

Troy Hunt
@troyhunt
Follow

@Black_DeckerUS is there a private channel I can report a serious security vulnerability on your website through? Or follow so I can DM.

Rui Silva
@ruisilva2015
Follow

@kickstarter Hi
I want to know how i can report a security vulnerability i have found on your website
Any email or something?
Thanks

esmile
@esmile_sec
Follow

@24hourfitness Do you guys have a security vulnerability disclosure program? I'd like to report a few things.

VDP Basics: Critical Elements

What's great about VDPs is they can be as simple as a few statements, and are generally just a few pages long. What's important is to include these five elements:

Promise:
You state a clear, good faith commitment to customers and other stakeholders potentially impacted by security vulnerabilities.

Scope:
You indicate what properties, products, and vulnerability types are covered.

"Safe Harbor":
Assures that the finder reporting in good faith will not be unduly penalized.

Process:
The process finders use to report vulnerabilities.

Preferences:
A living document that sets expectations for preferences and priorities regarding how reports will be evaluated.

Many VDP templates and guides exist; we recommend referencing the Coordinated Vulnerability Disclosure Template published by a working group of the U.S. National Telecommunications and Information Administration.

VDP Best Practices: Safe Harbor

Research shows that hackers sometimes avoid disclosing vulnerabilities due to non-existent or unclear disclosure policies. The risk of legal action is too great, they say, so the vulnerability remains open. To reassure hackers that, when acting in good faith, there will be no legal action, VDPs should include a safe harbor statement.

In March 2018, Dropbox made its VDP "a freely copyable template" for others to emulate. This is notable as Dropbox added a legal safe harbor pledge to its VDP, promising "to not initiate legal action for security research conducted pursuant to the policy, including good faith, accidental violations." HackerOne also introduced legal safe harbor language as a default for new policy pages, further solidifying it as industry standard.

VDP Basics: Those Leading the Way

No organization is too small or too large, too global or too local, to benefit from a VDP. And with VDPs becoming more important, many organizations are publicizing the details of their programs and policies. However, many more companies are still leaving themselves open to unnecessary risk.

Each year, HackerOne analyzes the entire Forbes Global 2000 list of the world's most valuable public companies as a benchmark for public VDP adoption. Based on the 2017 Forbes Global list, 93% of companies do not have a known VDP, compared to 94% of the 2016 list. While these numbers show marginal progress, there is significant room for improvement. With so many organizations urging companies to adopt VDPs, along with Gartner Research's recent predictions that 50% of enterprises will have crowdsourced security solutions by 2022 , we remain optimistic that more companies will publish VDPs soon.

But until VDP adoption increases, vulnerabilities will continue to go unreported, and breaches will continue to accelerate. Why? Because nearly 1 in 4 hackers have not reported a discovered vulnerability because the company didn't have a channel to disclose it, according to our 2018 Hacker Report.

Leading Companies Have Already Published VDPs

Progressive companies, regardless of industry or location, know the value of a public VDP. But many more companies still have not launched a VDP. These 50 companies, however, are just a sample of the Forbes Global 2000 who are leading the way with public VDPs:

ABB
Abbott Laboratories
Accenture
Alibaba
American Airlines Group
American Express
Apple
AT&T
Autodesk
BASF
Boston Scientific
British Sky Broadcasting
BT Group
Caterpillar
Citigroup
Comcast
Danske Bank
Deutsche Telekom
Eaton
Fiat Chrysler Automobiles
Garmin
General Electric
Honeywell International
Intel
Johnson & Johnson
Johnson Controls International
Mastercard
Medtronic
Oracle
Panasonic
Philips
PNC Financial Services
Royal Bank of Scotland
SAP
Schneider Electric
Smiths Group
Standard Chartered
Starbucks
Swisscom
Telecom Italia
Tencent Holding
Toyota Industries
Twenty-First Century Fox
Unilever
Visa
Vodafone
Walmart
Western Union
Yamaha Motors
ZTE

More Governing Bodies are Pushing VDPs

VDPs are seen as an invaluable tool in fighting cybercrime. Recently, government and industry organizations have begun to publish VDP templates, standards, and related guidance on how to implement, manage, and audit these important programs.

Standardization is being applied to VDPs by various bodies, with definitions published by the U.S. Department of Justice (DoJ) and in ISO 29147. Many other organizations have published guidance or issued statements including the U.S. Food & Drug Administration which said that "manufacturers should also adopt a coordinated vulnerability disclosure policy." Still others are positioning VDPs as an effective tool to help comply with laws and regulations, specifically GDPR.

The Center for European Policy Studies, for example, recently stated that VDPs "may reduce the risk of incurring fines arising from possible personal data breaches." This suggests that, in the case of a GDPR-related breach, the absence of a VDP could be seen as worthy of penalization.

Legal Experts and Market Leaders Tout VDP Value

"To improve the security of their connected systems, every corporation should have a vulnerability disclosure policy that allows them to receive security submissions from the outside world."

JEFF MASSIMILLA, VICE PRESIDENT GLOBAL CYBERSECURITY AT GM

"All companies should consider promulgating a vulnerability disclosure policy, that is, a public invitation for white hat security researchers to report vulnerabilities found on your system,"

ROD ROSENSTEIN, DEPUTY ATTORNEY GENERAL

"Companies that lack a clear vulnerability disclosure program are at increased risk should a security researcher find a vulnerability."

MEGAN BROWN, PARTNER, WILEY REIN LLP

Read what others had to say in Voices of Vulnerability Disclosure.

Governments and Industry Groups Continue to Promote VDPs

"We need to move to a world... where all companies providing internet services and devices adhere to a vulnerability disclosure policy."

"Vulnerability disclosure has long been an open, important issue in cybersecurity."

"Manufacturers should also adopt a coordinated vulnerability disclosure policy."

"Coordinated Vulnerability Disclosure...is mature and ready for inclusion in the (CVD) Framework."

"Automotive industry members should consider creating their own vulnerability reporting/ disclosure policies."

"The adoption of vulnerability disclosure policies represents a cost-effective and efficient method of identifying and addressing vulnerabilities."

"The private sector is responsible not only for developing the best possible software, but also for responsibly handling vulnerabilities whenever they are discovered."

How to Launch Your Own VDP

You're convinced of the value and security a VDP can bring to your organization, now all you need to do is get started.

If you're new to the concept of VDPs, we recommend you start by understanding the 5 critical components. Then, follow these 4 steps as you prepare for developing your own VDP.

#1: Get Stakeholders Involved

A VDP works well when it serves as the basis for a complete program and process for vulnerability reporting, disclosure, triage, resolution, communication, and metrics. A complete program means more than just the security team is involved.

At the very least, engineering, legal, product, and others should be consulted when developing your complete program. Furthermore, related to compliance, the Center for European Policy Studies recently stated that VDPs "may reduce the risk of incurring fines arising from possible personal data breaches." In other words, the absence of a VDP could be seen as worthy of penalization under GDPR, so your compliance teams should be involved as well.

Even minor issues can impact multiple teams, and major issues can disrupt an entire organization for months.

Consider the organizational implications of an incoming vulnerability report. Regardless of how the report is received, it has to get into the correct reporting and evaluation systems, and then be followed-up on and triaged by the appropriate teams. Then...

- Security needs to evaluate the implications, determine a course of action, communicate back to the finders, and determine any disclosure protocol.
- Product, development, engineering, and maybe even third-party vendors need to determine the severity, design a fix, and plan the resolution.
- Legal needs to be aware, in case of potential breaches or likelihood of risk exposure.
- Compliance has to evaluate the risk, determine how it impacts any regulations, track the audit trail, and look for ways to mitigate similar issues in the future.
- Marketing and communications should be aware of the potential for public disclosure or the impact on the organization's market, customers, and partners.
- Executives, partners, and customers may need to be briefed on the vulnerability, cost and scope of resolution, and potential fallout.

Even minor issues can impact multiple teams, and major issues can disrupt an entire organization for months. This isn't meant to scare you, it's meant to prompt you to be realistic and thorough as you build the program and processes around your VDP.

The point here is that VDPs aren't just a concern of the security team. It's critical to get other teams on board, aware of the importance of your VDP, and committed to publishing it and applying resources to the surrounding process.

#2: Build Internal Support

Convincing others in your organization may be a challenge, but there are plenty of resources available to help you build your case. Some include the many "Voices of VDP", from government agencies to attorneys to industry organizations who promote the benefits of vulnerability disclosure. Also, look to those companies leading the charge to push VDPs, like Dropbox and their recent move to make their own VDP a freely copyable template for others.

One particularly in-depth resource is The CERT Guide to Coordinated Vulnerability Disclosure, developed by the CERT Coordination Center at Carnegie Mellon University's Software Engineering Institute (SEI). Their guide explains the need for coordinated vulnerability disclosure (CVD), and more importantly, who should be involved. It's a thick read at over 100 pages, but we've distilled out the juicy bits in our "TL;DR Summary".

The benefit of thinking through a holistic VDP program means one thing: transparency. With the right communication and tracking processes in place, and the appropriate teams and individuals involved, risk is removed and there is less chance for surprises later in the process, or worse, long after you thought the process was complete.

#3: Pull It All Together

Our position, which reflects that of the wider industry, is pretty clear: properly implemented VDPs reduce risk.

However, launching a VDP is not as simple as "click here to launch your VDP". That's why we, and so many others, have published guides, templates, and more. We know that hacker-powered security is powerful, and we want the internet to be safer. More VDPs is a way to make that come true.

Deploying a VDP today is critical, especially as regulators and governing bodies increasingly see them as an expected component of every security apparatus. Not having one is no longer acceptable, and in fact, it's a detriment.

We're here to help. You can access ALL of our VDP-related content and posts right here. You can get details on HackerOne Response, the industry standard product trusted by The US Department of Defense, Goldman Sachs, General Motors, Adobe, and many more to securely and seamlessly receive and act on discovered vulnerabilities. To learn more and get a quick demonstration of what we offer, or simply ask us questions, contact us today or read on for more details.

#4: Use a Checklist

Building a thorough VDP program isn't trivial, but it need not be a long, onerous undertaking. As mentioned, there is a plethora of resources to help, and we've consolidated them into a helpful checklist. Use that resource as a guide, but obviously tailor the program to the nuances of your own organization and needs.

HERE ARE THE KEY AREAS TO COVER:

- ✔ Define your program
- ✔ Determine how you'll facilitate the program
- ✔ Build a program management team
- ✔ Consider public disclosure
- ✔ Drill down on internal processes, participants, and expectations
- ✔ Measure, report, and improve

The key to a successful VDP program is the underlying process. The process is what powers your VDP, so spending the time up front to develop and define it will save countless hiccups later. VDPs reduce risk, reduce managerial burdens, and accelerate overall business momentum, but only if done properly. This checklist is a great place to begin, as is the help of an experienced partner, like HackerOne.

VDPs reduce risk, reduce managerial burdens, and accelerate overall business momentum, but only if done properly.

Assembling the Right Tools to Support a VDP

When someone discovers a potential vulnerability on your website or in your products today, the lack of an easy-to-find VDP means you'll probably never know, or worse, others will know before you do. But, even if a hacker does manage to contact your organization, the lack of a structured process typically adds delays, or may even prevent the report from ever reaching the appropriate teams.

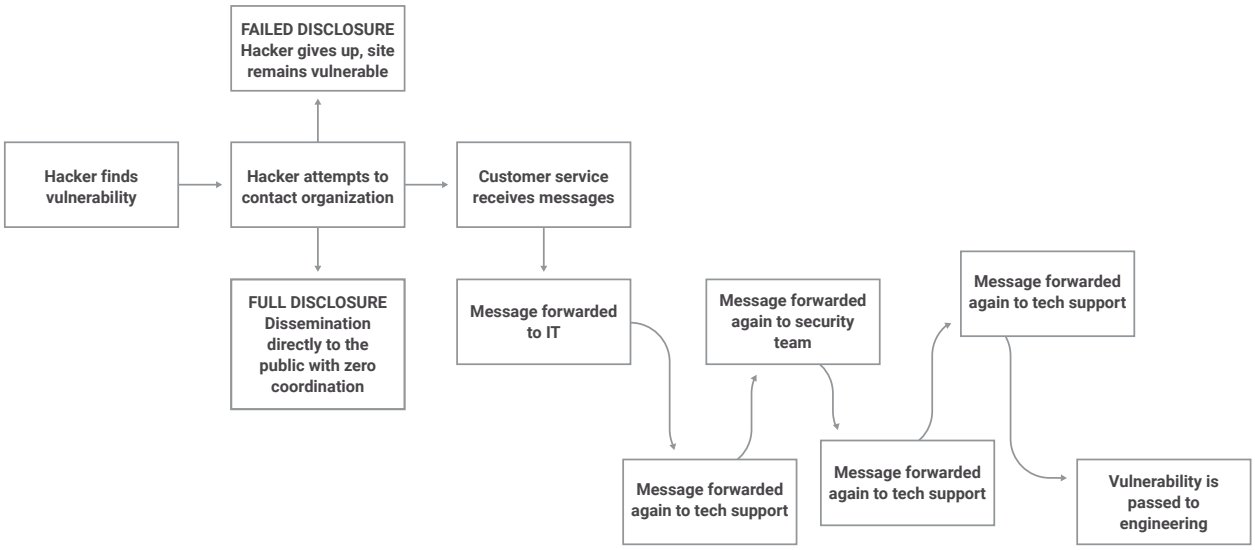
Ad Hoc Solutions Add Risk

The key to any reporting system is getting the incoming reports into the hands of the right people as fast and efficiently as possible.

Many organizations choose to use a security@myorganization[dot]com email address as their VDP's reporting method. They rely on a revolving team to check and appropriately triage incoming emails, then copy and paste that information into another reporting or bug tracking system. Still others might use a customer support solution to manage incoming reports, relying on the system and the customer support staff to appropriately route and track security-related messages.

These manual, ad hoc solutions take tools designed for other teams and other types of communications and try to apply them to a highly technical, highly specific task. They rely on decision-making from non-security workers, error-prone manual data transfers, and faith that the process won't lose or delay the discovery of a catastrophic vulnerability.

The Chaotic Nature of an Ad Hoc VDP Reporting Solution



With multiple points of contact and modes of communication, including email, social media, customer support channels, and even purpose-built reporting platforms, you risk losing track of valuable vulnerabilities unless personnel at every potential touchpoint are adequately trained on what to do when they receive a report.

Even then, when reports arrive via these unconventional channels, they risk being delayed or lost before the appropriate teams are alerted. Those precious days or weeks could be the difference between proactively resolving a vulnerability and protecting your brand, customers, and data, or allowing a security breach and the related fallout and penalties.

Auditing and Compliance

Furthermore, with security and data issues under the microscope more often than ever before, the issue of auditing and compliance add even more stress to an already fragile setup. Risk and compliance professionals know the value of having in place a defined process with easy-to-understand documentation and robust controls to manage users and their access.

Relying on an ad hoc vulnerability reporting system adds unnecessary risk to a process designed to minimize risk and maximize speed. A solution with built in compliance is the obvious way to go.

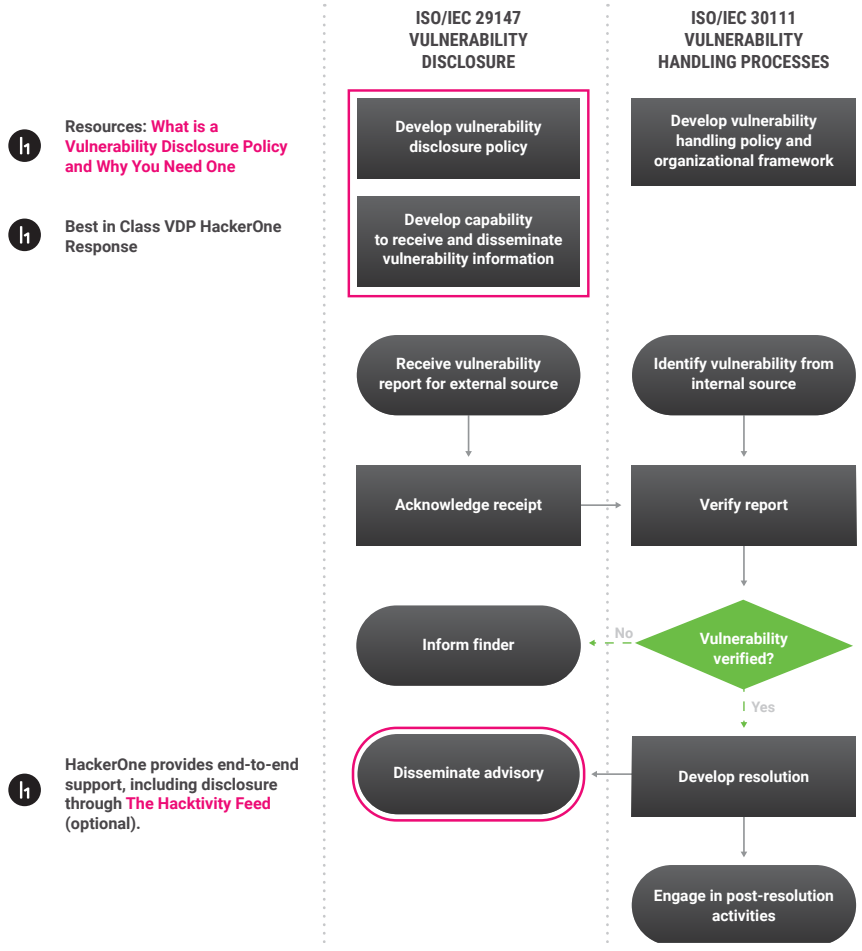
Auditability and compliance are critical, as VDPs and their accompanying audit trails are now seen as vital components of any modern compliance engine, especially in the age of GDPR. The Centre for European Policy Studies (CEPS) initiated a task force to define vulnerability disclosure guidelines for the European Union. Their recommendations state that since "irresponsible handling of vulnerabilities could lead to personal data breaches falling within the scope of GDPR", VDPs should be seen as one of the "necessary tools to mitigate the relevant risks."

Being compliant with ISO 29147 and SOC 2, especially for cloud-based service providers, is also increasingly important, and compliance with EU-U.S. and Swiss-U.S. Privacy Shield Frameworks offers additional data accountability. The resulting process tracking, auditability, conversation threads, and contextual vulnerability information keeps both reviewers and auditors happy.

Streamline Your VDP with HackerOne Response

HackerOne Response is our turnkey solution offering enterprise-grade security and conformance with ISO-29147 (vulnerability disclosure) and ISO-30111 (vulnerability handling). It allows SOC and Incident Response teams to work directly with external third-parties to resolve critical security vulnerabilities before they can be exploited. HackerOne Response provides a secure platform and integrates easily with existing systems and workflows.

High Level Overview of ISO-29147 (vulnerability disclosure) and ISO-30111 (vulnerability handling)

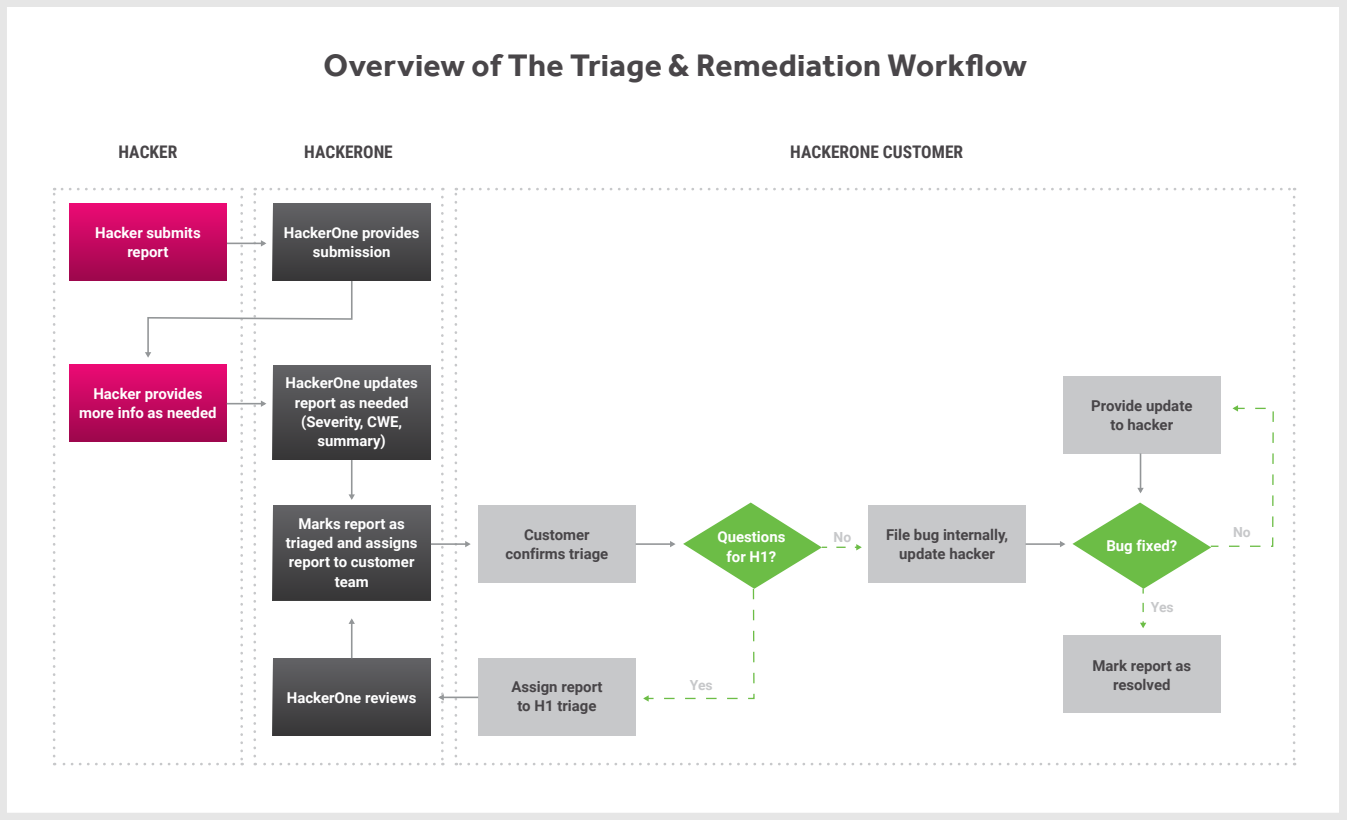


HackerOne Response enables you to have a single source of truth for all incoming vulnerability reports and their related activities. Your disclosure policy is published on HackerOne. Reports are submitted and managed via the same platform.

Assessments, reviews, and all related communications remain in one secure inbox. Data can be easily transferred in or out of HackerOne Response to and from your existing bug tracking, project management, or other tools with the HackerOne API. Once vulnerabilities are resolved, you can even publicly disclose reports via HackerOne if you choose to.

We even provide experienced triage teams to help support your staff and ease the burden of report management, categorization, and response.

Here's the breakdown of how it looks with HackerOne's Managed Services team handling the triage work for you.



With HackerOne's structured approach to vulnerability reporting and our expert guidance, you can streamline your existing process and build a faster, more dependable receipt and resolution machine.

Reduce Risk While Accelerating Resolution

HackerOne Response is a single solution that helps you simplify your disclosure process, reduce risk across your organization, and avoid the unpleasant surprise of an unknown vulnerability going public or getting exploited.

But HackerOne Response also elevates the experience for the finders as well. It not only gives them a clear and simple method for reporting potential bugs, it allows you to respond to and communicate with them with ease. Simply responding to them with acknowledgment of receipt is something few ad hoc solutions can guarantee. Furthermore, requesting more information or communicating with reporters on disclosure timelines is far easier through a dedicated system. Reporters have a one-stop location to see the status of their report and all related communications.

But all of this assumes you already have a process in place for receiving and managing incoming reports. If you're still not at that point, or if your current process is inadequate, HackerOne can help there, too.

HackerOne's vast experience, such as working with Auto-ISAC to offer VDP workshops and other Fortune 500 companies, is available to help you build or improve your VDP process, or to educate your industry. We've also published hundreds of vulnerability disclosure policies, and work closely with organizations of all sizes and across industries to publish vulnerability reports.

Our team will walk you through how best to craft a policy, what to expect in your first few months, and why our platform is far superior to other alternatives. Your team will never walk alone—whether facing critical vulnerabilities or curious reporters. Our customers also have access to communications support, technical assistance, hacker mediation, and more.

HackerOne's leadership and advocacy of VDPs had also resulted in the creation of a clearinghouse for related expertise and thought leadership. Our growing library of resources, created by our internal team as well as various government agencies, industry groups, and academia, is available to help answer questions and provide guidance to all.

Get Started

HackerOne Response lets you establish an ISO 29147-compliant vulnerability disclosure and assessment process for safely receiving and acting on vulnerabilities discovered by outside parties. Our purpose-built solution integrates easily with existing workflows, and, when you need extra help, lets our experienced triage team do the heavy-lifting.

To learn more, contact HackerOne today.

About HackerOne

HackerOne is the #1 hacker-powered security platform, helping organizations find and fix critical vulnerabilities before they can be exploited. More Fortune 500 and Forbes Global 1000 companies trust HackerOne than any other hacker-powered security alternative. The U.S. Department of Defense, General Motors, Google, Twitter, GitHub, Nintendo, Lufthansa, Panasonic Avionics, Qualcomm, Starbucks, Dropbox, Intel, the CERT Coordination Center and over 1,200 other organizations have partnered with HackerOne to resolve over 83,000 vulnerabilities and award over $38M in bug bounties. HackerOne is headquartered in San Francisco with offices in London, New York, the Netherlands, and Singapore.

For a comprehensive look at the industry based on the largest repository of hacker reported vulnerability data, download the The Hacker-Powered Security Report 2018.