

FROM OBLIGATION TO OPPORTUNITY

# A CISO's guide to vulnerability disclosure policies

Driving transparency with  
responsible disclosure



# Table of contents

- 4 Introduction
- 5 What is a vulnerability disclosure policy?
- 6 Why is having a VDP important?
- 8 What to include in your policy
- 10 Where to host a VDP
- 15 About Intigriti
- 16 Contact us





# Introduction

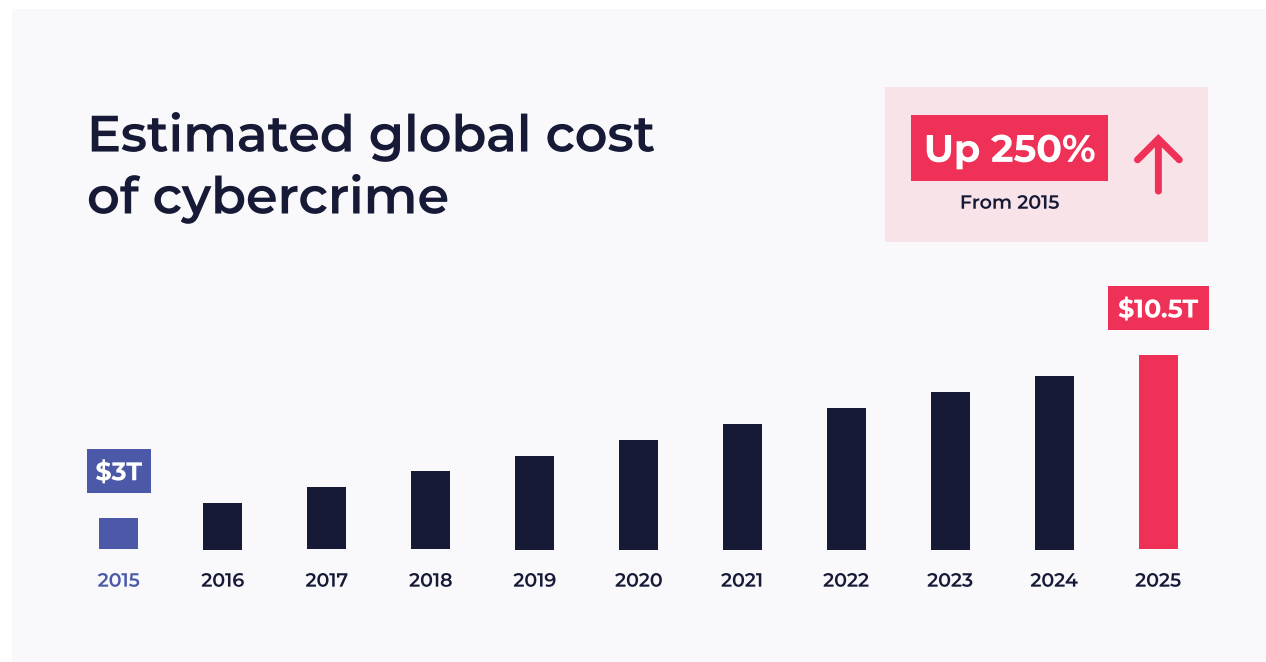
**By 2025, cybercrime is projected to take a staggering toll of \$10.5 trillion annually on global enterprises<sup>1</sup>, soaring from \$3 trillion in 2015. This exponential escalation, with a consistent year-over-year growth rate of 15%, underscores the relentless onslaught of digital threats facing organizations worldwide.**

Vulnerability is an omnipresent reality—it's an uncomfortable truth, but one CISOs must accept. With each technological advancement, organizations open new doors to innovation and progress, but simultaneously, they expose themselves to unprecedented risks and cyber threats.

In the face of these evolving threats, organizations must adopt a proactive approach to cybersecurity. It's no longer enough to merely react to incidents as they occur; we must anticipate and preempt potential vulnerabilities before they can be exploited. This is where Vulnerability Disclosure Policies (VDPs) emerge as a critical anchor in our defense strategy.

In the pages that follow, we will explore the indispensable role of VDPs in fortifying organizational defenses, meeting compliance standards, and

fostering a culture of responsible disclosure. Through real-world examples, best practices, and actionable insights, we will empower your organization to navigate the complex terrain of cybersecurity with confidence and resilience.



<sup>1</sup>[go.intigriti.com/cybercrime-cost-by-2025](https://go.intigriti.com/cybercrime-cost-by-2025)



# What is a vulnerability disclosure policy?

A vulnerability disclosure policy (VDP), also known as responsible disclosure, is a documented set of guidelines and procedures that an organization establishes to define how it handles reports of vulnerabilities in its systems, applications, or products. It serves as a framework for ethical hackers, security researchers, or any external party to responsibly disclose identified vulnerabilities to the organization.

The primary purpose of a VDP is to encourage the responsible reporting of vulnerabilities and establish a clear and transparent process for their **disclosure**, **assessment**, and **remediation**. It provides a channel for security researchers to report vulnerabilities without fear of legal repercussions, as long as they adhere to the guidelines outlined in the policy.

## By implementing a well-crafted vulnerability disclosure policy, organizations can:

- › Foster a positive relationship with the security researcher community
- › Encourage responsible reporting
- › Improve their overall security posture by addressing vulnerabilities before they can be exploited by malicious actors

RESEARCHER

Vampire01





# Why is having a VDP important?

**A VDP harnesses the power of crowdsourcing by creating an open channel for ethical hackers to work with your security team. Here are some other key reasons why having one is critical for tackling today's threat landscape.**

## **1. Encourages responsible reporting**

A VDP provides a clear and defined process for security researchers and ethical hackers to report vulnerabilities they discover responsibly. It establishes a channel for them to disclose vulnerabilities without resorting to public disclosure.

## **2. Enhances security posture**

A VDP allows organizations to identify and address vulnerabilities before they can be exploited by malicious actors. By receiving reports from external parties, organizations can leverage the expertise of security researchers to identify weaknesses that may have been overlooked during internal security assessments.

## **3. Demonstrates commitment to security**

Implementing a VDP demonstrates an organization's commitment to security and its willingness to work

collaboratively with the security community. It sends a message that the organization takes security seriously and values the contributions of ethical hackers and researchers. This can enhance the organization's reputation and build trust between customers, partners, and stakeholders.

## **4. Legal compliance**

Compliance frameworks such as GDPR, HIPAA, PCI DSS, and others mandate stringent requirements for data protection and security. Implementing a robust VDP not only aligns with these standards but also demonstrates a commitment to transparency, accountability, and proactive risk management.

## **5. Mitigates legal risks**

By clearly defining the rules of engagement and providing safe harbor provisions, organizations can establish a legal framework that protects both

the organization and the security researchers.

This can help prevent potential legal disputes and encourage more researchers to responsibly disclose vulnerabilities.

## **6. Collaboration with the security community**

A VDP fosters collaboration between organizations and the security community. It encourages open communication, knowledge sharing, and the exchange of best practices. By engaging with the security community, organizations can tap into a vast pool of expertise and stay informed about emerging threats and vulnerabilities.



# Vulnerability disclosure statistics

## Without a VDP, 44% of vulnerability submissions aren't successfully reported

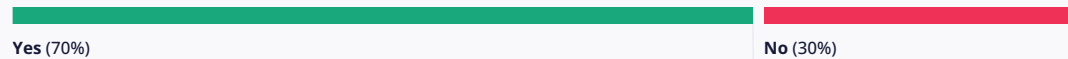
We asked our community how they report vulnerabilities outside a bug bounty program. Concerningly, 70% have identified vulnerabilities before but found no vulnerable disclosure program to report it. Of that group, 12% didn't escalate the

report. For those that did, 32% of them said the report got lost in the process or they weren't sure whether it was successfully reported. That's 44% of the risks that remain undetected.

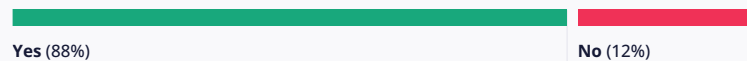
**i** Deploying a VDP will help lower the risk of a vulnerability not reaching your security team or getting published publicly (such as on social media).



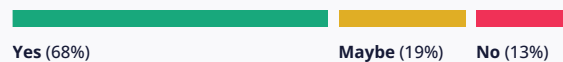
Have you ever found a vulnerability in a company without a hacker policy?



Did you report this vulnerability?



Was your report successful?





# What to include in your policy

A well-defined VDP typically includes the following elements:





**i** Tip! Head to Intigriti's website to see examples of **responsible disclosure policies**<sup>2</sup>. Alternatively, numerous online sources offer VDP templates for organizations to use. For example, **The Coordinated Vulnerability Disclosure Template**<sup>3</sup>, published by a working group of the U.S. National Telecommunications and Information Administration.

**07 • Remediation and disclosure**

Outline the steps the organization will take to address and remediate the reported vulnerabilities, including timelines for fixes and subsequent disclosure to the public.

**09 • Communication and transparency**

Emphasize your organization's commitment to maintaining open and transparent communication with reporters throughout the vulnerability disclosure process.

**08 • Legal considerations**

Clarify any legal protections or safe harbor provisions offered to security researchers who adhere to the policy's guidelines.



<sup>2</sup>[go.intigriti.com/programs-1](https://go.intigriti.com/programs-1)

<sup>3</sup>[go.intigriti.com/coordinated-vulnerability-disclosure-template](https://go.intigriti.com/coordinated-vulnerability-disclosure-template)



# Where to host a VDP

## On your website

Hosting a VDP on your own website has both pros and cons. Here are some considerations:

### Pros

#### Branding and transparency

Hosting your policy on your website maintains branding consistency and alignment with your organization's values, enhancing transparency and building trust with security researchers and stakeholders.

#### Control

Hosting your VDP or RDP on your own website gives you full control over the content, format, and processes. You can tailor it to your organization's specific needs and requirements.

#### Direct communication

Hosting a VDP on your website enables direct communication with security researchers, offering a clear channel for vulnerability reporting and facilitating interaction for clarification.

#### Integration with internal processes

Hosting your VDP on your website integrates with internal vulnerability management, aligning reporting and remediation workflows with incident response and security operations procedures.





## Cons

### Limited reach

Hosting your VDP on your website might limit its visibility. Researchers may prefer reporting through bug bounty platforms for broader exposure and potential rewards.

### Resource-intensive

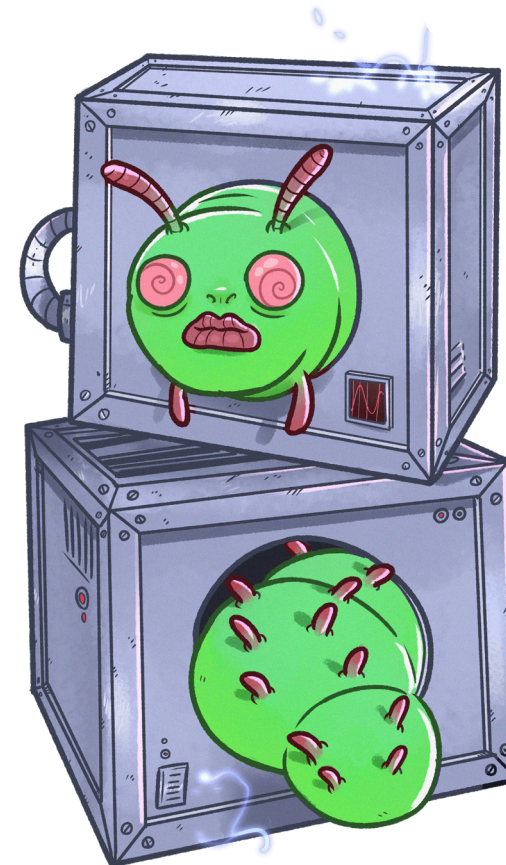
Hosting your VDP on your website demands dedicated resources for triaging, validating reports, responding to inquiries, and coordinating remediation. This creates challenges for organizations with limited security expertise.

### Lack of triage support

Bug bounty platforms typically offer their own security experts for triaging reports, unlike hosting your policy internally, which ordinarily requires your security team to handle validation.

### Reputation management

Hosting the VDP or RDP on your own website puts the responsibility of managing the reputation and credibility of the program solely on your organization. Any mishandling or miscommunication can impact your organization's reputation among security researchers.





## Using a bug bounty platform

### Pros

#### Centralized reporting

Hosting your VDP on a bug bounty platform centralizes reporting, streamlining the process and ensuring proper documentation and tracking of vulnerability submissions.

#### Access to skilled researchers

Bug bounty platforms attract highly talented, proactive ethical researchers with a wide range of skillsets. Hosting your VDP there provides access to this community, enhancing vulnerability discovery and mitigation.

#### Scalability

Bug bounty platforms manage large-scale vulnerability reporting efficiently with infrastructure and processes in place. They triage, validate, and address submissions promptly.

#### Expert triage and validation

Bug bounty platforms offer in-house security experts for triaging and validating vulnerability reports, lessening the load on your internal team. Intigriti includes this service with all programs, at no additional expense.

#### Collaboration and communication

Hosting your VDP on a bug bounty platform fosters effective communication and collaboration with security researchers in a secure, structured environment for exchanging information and addressing concerns.

#### Incentivizing researchers

Bug bounty platforms incentivize researchers with monetary rewards for reporting valid vulnerabilities, motivating active participation in your VDP and increasing critical vulnerability discovery.

#### Reputation enhancement

Hosting your VDP on a trusted bug bounty platform showcases your commitment to security and responsible vulnerability management, enhancing your reputation among researchers, customers, and stakeholders.



## Cons

### Platform dependency

Hosting your VDP solely on a bug bounty platform means relying on the platform's infrastructure and processes.

### Limited control

The policy may need to adhere to the platform's guidelines and requirements.

### Platform reputation

The reputation and credibility of the bug bounty platform hosting your VDP can reflect on your organization. Choosing a reputable platform with a strong track record is important to maintain trust with security researchers and stakeholders.

## Cost

Bug bounty platforms typically charge fees for their services, including hosting your VDP. Depending on your organization's budget and resources, this cost may be a consideration.

It's worth noting that organizations can adopt a hybrid approach by hosting their VDP on their website while also collaborating with bug bounty platforms or other third-party channels. This allows for broader coverage and engagement with the security research community while maintaining control over the disclosure process.





## VDP supports compliance requirements

**Having a Vulnerability Disclosure Policy (VDP) can help organizations meet various compliance processes and regulations, including:**

**GDPR (EU):** The General Data Protection Regulation (GDPR) mandates appropriate security measures to protect personal data. A VDP demonstrates a commitment to security and proactive vulnerability management, aligning with GDPR requirements.

**ISO 27001:** The ISO 27001 standard focuses on information security management systems. A VDP can contribute to its compliance by demonstrating that the organization has established processes for identifying and addressing security vulnerabilities.

**Cyber Resilience Act:** The Cyber Resilience Act is legislation that focuses on enhancing the resilience of organizations and critical infrastructure against cyber threats in Europe. While a VDP may not be explicitly required, having one will align with the spirit of the act by promoting proactive vulnerability management and collaboration with external parties.

**Digital Operations Resilience Act:** The Digital Operations Resilience Act, due to come into force in January 2025, will aim to achieve the resilience and security of digital operations, particularly in critical sectors. It will establish standards and requirements for organizations to protect their digital infrastructure, systems, and data from cyber

threats. A VDP will be seen as a proactive measure to identify and address vulnerabilities, contributing to the overall resilience of digital operations.

**NIST Cybersecurity Framework (US):** The NIST Cybersecurity Framework provides guidelines for managing cybersecurity risks. A VDP aligns with the framework by promoting proactive vulnerability management and collaboration with external parties.

**PCI DSS:** The Payment Card Industry Data Security Standard (PCI DSS) requires a secure environment for payment card data. Implementing a VDP demonstrates a commitment to identifying and addressing vulnerabilities that impact payment card data security.

**HIPAA:** The Health Insurance Portability and Accountability Act (HIPAA) sets standards for protecting sensitive health information. While not explicitly required, a VDP contributes to compliance by demonstrating a commitment to security and vulnerability management.

**CCPA:** The California Consumer Privacy Act (CCPA) grants rights regarding personal information. Implementing a VDP contributes to compliance

by protecting personal data and addressing vulnerabilities promptly.

**PSTI Act (EU):** Organizations are required to have robust security practices in place as part of the PSTI Act. A VDP is essential to these practices, as it outlines the organization's vulnerability management and disclosure approach.

**SOX (Sarbanes-Oxley Act):** SOX mandates financial reporting and internal control requirements. While not explicitly required, a VDP demonstrates a commitment to effective internal controls and addressing security vulnerabilities.

**PSD2:** Revised Payment Services Directive (PSD2) regulates payment services and enhances security. Implementing a VDP demonstrates a proactive approach to identifying and addressing vulnerabilities in payment systems and customer data.

**GLBA:** The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to protect customer information. While not mandated, a VDP contributes to compliance by identifying and addressing vulnerabilities impacting customer data security.



# About Intigriti

**Intigriti is a rapidly growing cybersecurity company that specializes in crowdsourced security services to help organizations protect themselves from cybercrime.**

Founded in 2016, Intigriti now has a global team of 100+ employees spread across Belgium, the United Kingdom, the Netherlands, and South Africa. And with the backing of our recent Series B Funding, we're planning on taking our growth to the next level.

**Agile security testing  
powered by the crowd**



## What to expect as an Intigriti customer

### Conquer the limitations of traditional security testing

Continuously test your digital assets for vulnerabilities by leveraging the expertise of Intigriti's 100,000+ registered security researchers.

### Industry-leading support

Only receive unknown, unique, valid, and in-scope vulnerability reports—all submissions are rigorously assessed by our dedicated triage team before we transmit them to the client. This enables your team to stay focused on business-critical tasks. Our offering includes triage, account management, customer success, knowledge base, technical support, and more.

### Reduced risk

On average, Intigriti clients receive 53 vulnerability reports within one week of launching a bug bounty program through our platform. Intigriti's support empowers organizations to identify and remediate risks quickly.

### Customized pricing

We provide a scalable model that aligns with customer aspirations and program expansion. Clients of all sizes and from various business sectors use our services.

Information from Q4/2024. We are constantly growing, so please contact our sales department or see our website for an accurate number.



## Contact us

**Need some help getting started with ethical hackers?**  
**Our experts can help you maximize the success of your bug bounty program. Get in touch today to connect with the brightest and most experienced researchers across the globe.**

[www.intigriti.com](http://www.intigriti.com)

[hello@intigriti.com](mailto:hello@intigriti.com)

 Intigriti  [hackwithintigriti](#)  [@intigriti](#)  [Intigriti](#)  [Intigriti](#)

Illustrations by [Zwoltopia](#)

