Vulnerability Disclosure Policies (VDP):
Guidance for Financial Services
5 Critical Components to Getting It Right

As security incidents increase in frequency — and regulators begin taking closer notice — the pressure placed on security leaders in the financial services sector is mounting.

According to a 2018 PwC report, the number and range of vulnerabilities are growing as finserv organizations outsource internal processes, shift computing to the cloud, and connect to customers through more channels than ever before. While financial firms benefit from digital networking, this also enlarges their "attack surface" exposed to criminal hackers. With more than eight billion connected "things" in the wild, there are now more networked endpoints in the world than there are people.

But hope is not lost. By recognizing that criminals can — and will — discover new vulnerabilities in nearly any software, application, or network surface they access, leaders can quickly and confidently shift their security strategy to an offensive approach, enabling them to beat criminals at their own game and reduce the risk of a serious security incident.
Now is the time to act.

In 2018, all financial services firms — regardless of location or size — need to draft and publish a clear vulnerability disclosure policy (VDP) to effectively partner with the creative and intelligent security community and reduce the risk of a security incident by finding and fixing critical security vulnerabilities before they fall into the wrong hands.

Regardless of where and how you publish your VDP — on HackerOne or as a standalone policy on your organization’s website - the time is now to join leaders in the financial services sector, such as Goldman Sachs and American Express, and prioritize a vulnerability disclosure policy for your organization in 2018.

The International Organization for Standardization, ISO/IEC 29147:2014 has also provided guidelines for the disclosure of potential vulnerabilities in products and online services. Specifically, it details the methods a vendor should use to address issues related to vulnerability disclosure.

This document was created to help you understand the critical elements of designing an effective vulnerability disclosure policy at your institution.

Guidance on vulnerability disclosure has been published by numerous organizations, including:

- United States Department of Defense
- National Institute of Standards and Technology
- Federal Trade Commission
- Food and Drug Administration
- National Telecommunications and Information Administration
- National Highway Traffic Safety Administration
What is a Vulnerability Disclosure Policy?

A vulnerability disclosure policy, or VDP, is intended to give ethical hackers clear guidelines for submitting potentially unknown and harmful security vulnerabilities to organizations. A VDP allows you to have a clear communication mechanism in place for the people who are interested in reporting vulnerabilities in your products and services.

Megan Brown, Partner at Wiley Rein LLP, said in a recent webinar, “Companies that lack a clear vulnerability disclosure program are at increased risk should a security researcher find a vulnerability.”

In December 2016, the NTIA published a Coordinated Vulnerability Disclosure Template, the result of a working group that included representatives from HackerOne. The jointly created template is the basis for our guidance.

Effective VDPs need not be long, but generally must contain five key elements:

1. **Promise:** Demonstrate a clear, good faith commitment to customers and other stakeholders potentially impacted by security vulnerabilities.

2. **Scope:** Indicate what properties, products, and vulnerability types are covered.

3. **“Safe Harbor”:** Assures that reporters of good faith will not be unduly penalized.

4. **Process:** The process finders use to report vulnerabilities.

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

A well-considered VDP serves as the basis for a complete vulnerability disclosure program, which defines how organizations handle incoming alerts (legally and technically), how they communicate with finders, how their internal teams validate, mitigate, and externally disclose a security vulnerability, and how activities and results are summarized and reported to stakeholders and decision-makers.
Vulnerability Disclosure Policy Basics: 5 Critical Components

1. Promise
Demonstrate a clear, good faith commitment to customers and other stakeholders potentially impacted by security vulnerabilities.

The opening section of a VDP conveys the mission behind the policy’s creation. NTIA refers to this opening section as the “brand promise,” explaining the organization’s commitment to security, customers, and others. The audience for this section is customers and the overall marketplace, such as partners, competitors, regulators, and the media.

The commitment should include statements on why this policy was created, why it is important to have a public policy, what it is expected to accomplish. Additionally, it may include specific statements to customers and to finders communicating the importance of the program, the intent, and the value of working with the security community.

From the U.S. Department of Defense’s VDP:

Maintaining the security of our networks is a high priority at the DoD. Our information technologies provide critical services to Military Service members, their families, and DoD employees and contractors. Ultimately, our network security ensures that we can accomplish our missions and defend the United States of America.

The security researcher community regularly makes valuable contributions to the security of organizations and the broader Internet, and DoD recognizes that fostering a close relationship with the community will help improve our own security. So if you have information about a vulnerability in a DoD website or web application, we want to hear from you!
2. Scope
Indicate what properties, products, and vulnerability types are covered.

It is directed at finders, helping to guide their efforts by specifying what is fair game or where particular attention is requested or not allowed. For types of vulnerabilities, it may state which are worthy of report, and may exclude others which might be obvious or serve as merely noise related to the larger goals of the program.

For clarity, this section should include both what is in scope and what is out of scope. Limitations may be put on which product or software versions are fair game, since older versions may be beyond their lifecycle or no longer supported. Organizations may also choose to keep certain systems or products off limits to protect customer data or intellectual property.

For example, the Goldman Sachs VDP encourages submissions for all three (3) main webapp properties owned by Goldman Sachs but explicitly excludes things such as non-https domains and vulnerabilities affecting outdated browsers:

**In-Scope**

- *.gs.com
- *.goldman.com
- *.goldmansachs.com
3. "Safe Harbor"

Assures that reporters of good faith will not be unduly penalized. It essentially says, "we will not take legal action if..."

Any individual who willingly participates in a vulnerability disclosure process is subjecting themselves to undue risk. As a result, one of the most critical components of any policy is a clear, unambiguous statement that good faith efforts will not result in you initiating legal action.

To these finders disclosing vulnerabilities in good faith, the language should be inviting, non-threatening, clear, and, as NTIA states, "more affirmative than prohibitive." NTIA further recommends using a simple phrase like, "If you follow these guidelines we will not pursue or support any legal action related to your research." In general, your goal is to create a "safe harbor" that demonstrates good faith and builds trust.

From Salesforce.com VDP

"Salesforce pledges not to initiate legal action against researchers ... as long as they adhere to this policy."
4. Process

The process finders use to report vulnerabilities — how to submit their reports and what information is requested.

State the mechanism for submission, whether via email or a secure web form or another means. It should also state which specific details of the vulnerability should be included in the submission.

Remember that finders are unpaid, so the request for information is just that: a request. Keep in mind, requiring too much information may result in less submissions. One note on the form-factor for receiving these vulnerabilities, accepting an email submission may result in absent or unstructured information, while a secure web form can specify required and optional or helpful information. This is where HackerOne Response can significantly streamline your disclosure process.

From NTIA Template

How to Submit a Vulnerability

To submit a vulnerability report to ACME’s Product Security Team, please utilize the following form <link to vulnerability reporting form>.

What we would like to see from you:

- Well-written reports in English will have a higher chance of being accepted.
- Reports that include proof of concept code will be more likely to be accepted.
- Reports that include only crash dumps or other automated tool output will most likely not be accepted.
- Reports that include products not on the covered list will most likely be ignored.
- Include how you found the bug, the impact, and any potential remediation.
- Any plans for public disclosure.

What you can expect from us:

- A timely response to your email (within 2 business days).
- An open dialog to discuss issues.
- Notification when the vulnerability analysis has completed each stage of our review.
- An expected timeline for patches and fixes (usually within 120 days).
- Credit after the vulnerability has been validated and fixed.
5. Preferences

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

This can include the expected duration between submission and initial response, confirmation of vulnerability, additional communications during remediation, expectation of recognition, and if or when finders have the permission to publicly disclose found vulnerabilities.

Since it should be clear that this section is non-binding, it is also recommended to include a general statement on the variability of timing based on bug severity, product, and other internal or external factors, to further set expectations on changes to the process timeline.

A reminder on public disclosure from the NTIA:

“Finders do not create vulnerabilities. The fact that one finder does not disclose its existence does not guarantee that another will not find it – or has not already found it. Finders may have reasons to want to disclose the vulnerability publicly. A [coordinated] disclosure situation is preferable to one without control. Vendors may want to express preferences on when finders publicly talk about vulnerabilities.”

Because reasonable people can disagree on the method and manner of public disclosure, it may also be prudent to have a defined path of escalation and mediation. Customers of HackerOne Response can benefit from a structured public disclosure process and our mediation assistance.

This again underscores the importance of a VDP, since it gives organizations the opportunity to request preferences on when finders can publicly disclose bugs, and can even provide reasoning for longer durations. This policy is an important step in guiding the vulnerability coordination efforts that are crucial to protecting consumers.

From Amazon Web Services Vulnerability Reporting Policy

Public Notification

If applicable, AWS will coordinate public notification of a validated vulnerability with you. When possible, we would prefer that our respective public disclosures be posted simultaneously.

In order to protect our customers, AWS requests that you not post or share any information about a potential vulnerability in any public setting until we have researched, responded to, and addressed the reported vulnerability and informed customers if needed.
Publishing Your Vulnerability Disclosure Policy

Once the policy is finalized and you are ready to accept submissions, it is time to publish the policy on an accessible, easy-to-find website.

In the past, most organizations published their vulnerability disclosure policy on their own website. Some organizations also included an email address specifically for submitting security issues. Many of these programs can be found in the HackerOne Directory, a community-curated resource for contacting security teams.

Now is the Time to Act

Dozens of organizations choose HackerOne to assist their VDP efforts. HackerOne Response provides auditable compliance with ISO-29147 (vulnerability disclosure) and ISO-30111 (vulnerability handling). The platform complements your application security efforts across multiple business units, including security operations, incident response, and red-teams. Customers have seen it reduce risk, simplify operations, save time and money, and overall improve security posture.

If you’re a risk officer, a clear policy mitigates the risk of unauthorized disclosure, illegal hacking, and adverse administrative or regulatory action.

"[Fandango] engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security... including: **Failing to maintain an adequate process for receiving and addressing security vulnerability reports from third parties.**"

- Complaint, Federal Trade Commission
For the CISO, you gain full visibility and control over what otherwise would be a chaotic process.

"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."

- Jeffrey Massimilla, Chief Product Cybersecurity Officer, General Motors

And security teams can sleep better at night knowing they have significantly improved the company’s security posture.

"We have pretty much almost every type of vulnerability come in. It is, I would say, unbelievably successful."

- Chris Lynch, Defense Digital Service Chief

General Counsels can rely on a policy-driven approach that limits the risk of extralegal public vulnerability leaks.

"Companies that lack a clear vulnerability disclosure program are at increased risk should a security researcher find a vulnerability, which then they may disclose in a chaotic manner."

- Megan L. Brown, Partner, Wiley Rein, LLP

And for other executives, a policy can provide additional ammunition to answer board, investor, and media inquiries around your cyber security risk posture.
"One of the best ways for us to augment our internal security team is to work with the white hat community."

- Tobias Lütke, CEO, Shopify

Many of the leading players across nearly every vertical have published vulnerability disclosure policies, yet it remains that 93% of the top global companies still do not have a VDP in place. As shown in this document, they are quickly becoming an established best practice and even a regulatory expectation.

By implementing a vulnerability disclosure policy, companies strengthen their security posture and reduce a key area of cybersecurity risk. Launching a VDP with HackerOne Response carries with it many benefits for you and your colleagues.

To learn more about HackerOne Response, contact your HackerOne account representative today.
Published Guidance on Vulnerability Disclosure

A Framework for a Vulnerability Disclosure Program for Online Systems
https://www.justice.gov/criminal-ccips/page/file/983996/download

Postmarket Management of Cybersecurity in Medical Devices Guidance for Industry and Food and Drug Administration Staff

Start With Security A Guide for Business

DoD Vulnerability Disclosure Policy
https://hackerone.com/deptofdefense

“Early Stage” Coordinated | Vulnerability Disclosure Template

What We Heard | The Cybersecurity Framework Workshop

Cybersecurity Best Practices for Modern Vehicles