HERE ARE THE 5 CRITICAL COMPONENTS OF A VULNERABILITY DISCLOSURE POLICY

Vulnerabilities are found in your technology every day by researchers, friendly hackers, journalists, and others. But do they have an obvious way to alert you when they find one? A vulnerability disclosure policy (VDP) gives ethical hackers clear guidelines for reporting potentially unknown and harmful security vulnerabilities. They don't need to be long nor should they require months to generate, but they should contain enough detail to help both you and the researchers improve your security.

PROMISE

Convey the mission behind the policy and explain your commitment to security, customers, and others. Include statements on why this policy was created, why it is important to have a public policy, what it is expected to accomplish.

SCOPE

Specify what is fair game, and where attention is requested or not allowed. Also state which types of vulnerabilities should be reported and which are excluded. Limitations may also be put on products or versions, or to protect data or intellectual property.

"SAFE HARBOR"

Write a good faith commitment that reporters will not be penalized. Essentially say, "we will not take legal action if..." This gives needed reassurance to those disclosing a vulnerability, so make the language inviting, non- threatening, and clear.

PROCESS

Detail how finders should submit reports and what information you would like to see. This also is where you can set expectations for subsequent communications. Requesting emailed reports can lead to incomplete and unstructured information, while a secure web form like HackerOne's Response product can ensure completeness.

PREFERENCES

Set non-binding expectations for how reports will be evaluated. This section can include the duration between submission and response, confirmation of vulnerability, follow-on communications, expectation of recognition, and if or when finders have permission to publicly disclose their findings.

HACKERONE RESPONSE

Dozens of organizations choose HackerOne Response to assist their VDP efforts. It provides auditable compliance, with capabilities to complement your security efforts across security operations, incident response, and red-teams. Our customers have seen it reduce risk, simplify operations, save time and money, and improve their overall security posture. To learn more about HackerOne Response, talk to a HackerOne representative today.

HackerOne Response Users

GM Adobe airbnb

hackerone

DOWNLOAD THE FREE EBOOK

To learn more about generating your own VDP, download our "Vulnerability Disclosure Policy Basics" ebook. It details each of these 5 critical components, gives examples of text from real VDPs, and provides recommendations from pioneering organizations.