JULY 2022

whitehat.ng

Vulnerability Disclosure Policy Template

Whitehat.NG – Pushing for responsible disclosure in Nigeria.

YOU SEE SOMETHING, SAY SOMETHING BUT RESPONSIBLY

Vulnerability Disclosure Policy Template – Outline

- Introduction
- Authorization
- Guidelines
- Scope
- Rule of Engagement
- Reporting a Vulnerability
- Disclosure
- Acknowledgment
- Questions

Introduction

[INSERT_COMPANY_NAME] is committed to ensuring the security of customers, users and employee by protecting their information from unwarranted disclosure. This policy is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and to convey our preferences in how to submit discovered vulnerabilities to us.

This policy describes what systems and types of research are covered under this policy, how to send us vulnerability reports, and how long we ask security researchers to wait before publicly disclosing vulnerabilities.

We want security researchers to feel comfortable reporting vulnerabilities they've discovered – as set out in this policy – so we can fix them and keep our users safe. We have developed this policy to reflect our values and uphold our sense of responsibility to security researchers who share their expertise with us in good faith.

An introductory section that provides background information about your organization and your VDP. It should take a committed, concerned, and receptive tone.

Authorization

- If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorized, we will work with you to understand and resolve the issue quickly, and [INSERT_COMPANY_NAME] will not recommend or pursue legal action related to your research.

- If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorized we will work with you to understand and resolve the issue quickly, and [INSERT_COMPANY_NAME] will not recommend or pursue legal action related to your research. Should legal action be initiated by a third party against you for activities that were conducted in accordance with this policy, we will make this authorization known.

This section reflects your commitment to not take legal action against anyone in the general public for security research activities that represent a good faith effort to follow the policy.

Guidelines

Under this policy, "research" means activities in which you:

- Notify us as soon as possible after you discover a real or potential security issue.
- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Only use exploits to the extent necessary to confirm a vulnerability's presence. Do not use an exploit to compromise or exfiltrate data, establish command line access and/or persistence, or use the exploit to "pivot" to other systems.
- Provide us a reasonable amount of time to resolve the issue before you disclose it publicly.
- You do not intentionally compromise the privacy or safety of [INSERT_COMPANY_NAME] personnel (e.g. employees) or any third parties.
- You do not intentionally compromise the intellectual property or other commercial or financial interests of any [INSERT_COMPANY_NAME] personnel or entities, or any third parties.

Once you've established that a vulnerability exists or encounter any sensitive data (including personally identifiable information, financial information, or proprietary information or trade secrets of any party), you must stop your test, notify us immediately, and not disclose this data to anyone else.

Scope

Systems and services associated with domains and sub-domains listed below are in scope. Additionally, any website published with a link to this policy shall be considered in scope. Websites not explicitly listed here or published with a link to this policy are considered out of scope for this policy.

Though we develop and maintain other internet-accessible systems or services, we ask that active research and testing only be conducted on the systems and services covered by the scope of this document. If there is a system not in scope that you think merits testing, please contact us to discuss it first. We will increase the scope of this policy over time.

This policy applies to the following systems and services: *allowlist*

This policy does not apply to the following systems and services: *denylist*

This section defines which internet-accessible systems or services are in scope of your policy. Your first published VDP must contain at least one production system or service, and it must also describe the types of tests that are allowed (or specifically not authorized).

Alternately, instead of an *allowlist* that enumerates which systems or services are in scope, you may choose to use a *denylist* to describe which are out of scope.

Before adding a system or service to the scope, ensure you are permitted to authorize security testing on the system or service. Specifically, if you, e.g., use a managed security service provider or SaaS, confirm whether the vendor has explicitly authorized such testing, such as in your organization's contract with the provider or their publicly available policy. If not, you should work with the vendor to obtain authorization

Rule of Engagement

Security researchers MUST NOT

- Test any system other than the systems set forth in the 'Scope' section above,
- Disclose vulnerability information except as set forth in the 'Reporting a Vulnerability' and 'Disclosure' sections below,
- Engage in physical testing of facilities or resources,
- Engage in social engineering,
- Send unsolicited electronic mail to [INSERT_COMPANY_NAME] users, employees, including "phishing" messages,
- Execute or attempt to execute "Denial of Service" or "Resource Exhaustion" attacks,
- Introduce malicious software,
- Test in a manner which could degrade the operation of [INSERT_COMPANY_NAME] systems; or intentionally impair, disrupt, or disable [INSERT_COMPANY_NAME] systems,
- Test third-party applications, websites, or services that integrate with or link to or from [INSERT_COMPANY_NAME] systems,
- Delete, alter, share, retain, or destroy [INSERT_COMPANY_NAME] data, or render [INSERT_COMPANY_NAME] data inaccessible, or,
- Use an exploit to exfiltrate data, establish command line access, establish a persistent presence on [INSERT_COMPANY_NAME] systems, or "pivot" to other [INSERT_COMPANY_NAME] systems.

Security researchers MAY:

- View or store [INSERT_COMPANY_NAME] nonpublic data only to the extent necessary to document the presence of a potential vulnerability.

Security researchers MUST:

- Cease testing and notify us immediately upon discovery of a vulnerability,
- Cease testing and notify us immediately upon discovery of an exposure of nonpublic data, and,
- Purge any stored [INSERT_COMPANY_NAME] nonpublic data upon reporting a vulnerability.

Reporting a Vulnerability

We accept vulnerability reports at [put_company_contact_email]. Reports may be submitted anonymously. We do not support PGP-encrypted emails at this time.

Information submitted under this policy will be used for defensive purposes only – to mitigate or remediate vulnerabilities. If your findings include newly discovered vulnerabilities that affect all users of a product or service and not solely [INSERT_COMPANY_NAME], we may share your report with the Nigeria Computer Emergency Response Team [NGCERT] where it will be handled. We will not share your name or contact information without express permission.

In order to help us triage and prioritize submissions, we recommend that your reports:

- Adhere to all legal terms and conditions outlined and the [INSERT_COMPANY_NAME] Responsible Disclosure Terms of Service .
- Describe the vulnerability, where it was discovered, and the potential impact of exploitation.
- Offer a detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts or screenshots are helpful).
- Be in English, if possible.

This section describes communication mechanisms and processes for submitting vulnerabilities. It must include instructions on where reports should be sent (e.g., a web form, email address), and a request for the information your agency needs to find and analyze the vulnerability (e.g., a description of the vulnerability, its location and potential impact; technical information needed to reproduce; any proof of concept code; etc.).

Disclosure

[INSERT_COMPANY_NAME] is committed to timely correction of vulnerabilities. However, we recognize that public disclosure of a vulnerability in absence of a readily available corrective action likely increases versus decreases risk.

Accordingly, we require that you refrain from sharing information about discovered vulnerabilities for 14 calendar days after you have received our acknowledgement of receipt of your report. If you believe others should be informed of the vulnerability prior to our implementation of corrective actions, we require that you coordinate in advance with us.

We may share vulnerability reports with the Nigeria CERT, as well as any affected vendors. We will not share names or contact data of security researchers unless given explicit permission.

This section describes what the organizations would like the researchers to do to ensure reported vulnerability have been fixed before final disclosure, and further guidance and choice can be provided.

Acknowledgement

For [INSERT_COMPANY_NAME], we appreciates the professionalism and support of all the security researchers who have helped [INSERT_COMPANY_NAME] securely deliver our mission. You can find our on our Acknowledgement Page [hyperlink] to see researchers who agreed to be publicly acknowledged for their effort.

What you can EXPECT from us

When you choose to share your contact information with us, we commit to coordinating with you as openly and as quickly as possible.

- Within 3 business days, we will acknowledge that your report has been received.
- To the best of our ability, we will confirm the existence of the vulnerability to you and be as transparent as possible about what steps we are taking during the remediation process, including on issues or challenges that may delay resolution.
- We will maintain an open dialogue to discuss issues.

If you operate a bug bounty program, you may consider referencing that in your VDP. For example, you could use language such as: “A subset of our systems may be eligible for bounties. Check out [hyperlink] for the current list of bounty-eligible systems.”

Questions

Questions regarding this policy may be sent to [INSERT_COMPANY_NAME] contact such as [email, phone number or Postal address]. We also invite you to contact us with suggestions for improving this policy.

Content created by the Security Team at [INSERT_COMPANY_NAME]
Content last reviewed [Month, Day and Year of Review]

Policy Document Change History can be tabulated as well down here to depict the version, date and descriptions of changes made during such review.

About Whitehat.NG

Founded in 2020, Whitehat Nigeria is composed of Nigeria Security Researchers whose motivations are patriotism, professionalism, and non-profit which intend to help reposition the cybersecurity posture of Nigeria by engaging in open security research of the Nation's cyberspace and report all sensitive findings to affected organizations. With the hope of forcing all organizations to adopt a Vulnerability Disclosure Policy (VDP) which will help ensure that the available attack surfaces for the adversary are being totally reduced. On the belief that until VDP adoption increases, vulnerabilities will continue to remain unreported, and breaches will continue at an accelerated rate, pushing for a managed disclosure situation which is preferable to one without control.

We encourage organizations with digital assets to use this template to put together their own unique VDP to encourage more vulnerability to be reported as nearly 1 in 4 hackers has not reported a discovered vulnerability because the company didn't have a channel to disclose it, according to 2018 Hacker Report from Hacker One.

For our continuous operation, we are going to be relying largely on the cooperation of all organizations in all sectors be it public or private to join hands and collaborate with us on great initiative. Support from members of the general public will be appreciated as we embark on this journey.

Thanks.

info@whitehat.ng
Whitehat.NG ngwhitehat

Examples of Vulnerability Disclosure Policies

U.S. Department of the Treasury
- https://home.treasury.gov/vulnerability-disclosure-policy

U.S. Department of Transportation
- https://www.transportation.gov/vulnerability-disclosure-policy

U.S. Department of Justice
- https://www.justice.gov/jmd/vulnerability-disclosure-policy

Bank of England
- https://www.bankofengland.co.uk/vulnerability-disclosure-policy

Deutsche Bank
- https://www.db.com/legal-resources/responsible-disclosure-process

Saxo Bank
- https://www.home.saxo/legal/vulnerability-disclosure-policy/vulnerability-disclosure-policy

Starling Bank
- https://www.starlingbank.com/security/disclosure/

JISC UK
- https://www.jisc.ac.uk/contact/vulnerability-disclosure-policy

NOMINET
- https://www.nominet.uk/vulnerability-disclosure-programme/

Evri
- https://www.evri.com/responsible-disclosure-policy

Names
- https://www.names.co.uk/info/company/vulnerability-disclosure

Boundary
- https://boundary.co.uk/vulnerability-disclosure-policy/

info@whitehat.ng
Whitehat.NG ngwhitehat