***Vulnerability Disclosure Policy Template***

*This template is intended to assist your agency in the creation of a vulnerability disclosure policy (VDP) that aligns with* [*Binding Operational Directive (BOD) 20-01*](https://cyber.dhs.gov/bod/20-01/)*.*

* *Instructions for how to use the template are provided throughout the document in red and italic text and should be removed from your published policy.*
* *You are encouraged to modify the template to suit your needs, but your policy must address all actions required by the Directive. It is* ***strongly recommended*** *that you use the template’s language for the Authorization section.*
* *CISA recommends that you review the* [*implementation guidance*](https://cyber.dhs.gov/bod/20-01/#compliance-guide) *maintained in support of this directive, particularly the section* [*Consider prior art*](https://cyber.dhs.gov/bod/20-01/#consider-prior-art)*.*
* *Your policy must be published as a web page and you must specify its location in your agency’s security.txt.*

*The primary sources for this template were the General Services Administration’s* [*Technology Transformation Services’ VDP*](https://18f.gsa.gov/vulnerability-disclosure-policy/)*, the* [*Department of Defense’s VDP*](https://hackerone.com/deptofdefense)*, and a VDP template from a 2016 working group of the* [*National Telecommunications and Information Administration*](https://www.ntia.doc.gov/files/ntia/publications/ntia_vuln_disclosure_early_stage_template.pdf)*. It has been written to align with the Department of Justice’s* [*Framework for a Vulnerability Disclosure Program for Online Systems*](https://www.justice.gov/criminal-ccips/page/file/983996/download)*.*

**Vulnerability Disclosure Policy**

*Agency Name*

*Month Day, Year*

# Introduction

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

*Agency Name* is committed to ensuring the security of the American public 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.

# Guidelines

We request that you:

* Notify us as soon as possible after you discover a real or potential security issue.
* Provide us a reasonable amount of time to resolve the issue before you disclose it publicly.
* 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.
* 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**.
* Do not submit a high volume of low-quality reports.

# Authorization

*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.*

*CISA* ***strongly encourages*** *keeping this language as-is. The language is designed to be as welcoming to researchers as possible, and to avoid “legalese” or other unnecessarily intimidating language.*

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 *Agency Name* will not recommend or pursue legal action related to your research.

# Scope

*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* ***blocklist*** *to describe which are out of scope.*

*Note:*

* *After your policy’s publication, all newly launched Internet-accessible systems or services must be included* implicitly *in the scope (e.g., by indicating a wildcard [\*] on a domain’s scope) or* explicitly *by updating the policy to account for these systems.*
* *At 2 years after the issuance of this directive, all internet-accessible systems or services must be in scope of your policy.*

This policy applies to the following systems and services:

* \*.agency-brand.gov
* agency-form.gov
* agency-service.gov, and the following hostnames:
  + alpaca.agency-service.gov
  + buffalo.agency-service.gov
  + cassowary.agency-service.gov
  + dormouse.agency-service.gov
  + Any other subdomain of agency-service.gov and all customer applications are excluded from this policy (\*.app.agency-service.gov is specifically excluded, except for \*.service-proxy.app.agency-service.gov.)
* Source code at https://github.com/agency-example/repo

**Any service not expressly listed above, such as any connected services, are excluded from scope** and are not authorized for testing. Additionally, vulnerabilities found in non-federal systems from our vendors fall outside of this policy’s scope and should be reported directly to the vendor according to their disclosure policy (if any). If you aren’t sure whether a system or endpoint is in scope or not, contact us at security@agency.gov before starting your research or at the security contact for the system’s domain name listed in the [.gov WHOIS](https://domains.dotgov.gov/dotgov-web/registration/whois.xhtml).

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 particular 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.

## Types of testing

**The following test types are not authorized:**

* Network denial of service (DoS or DDoS) tests
* Physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing

# Reporting a vulnerability

*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), 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.). Reporters must be allowed to submit a report anonymously: you must not require the submission of personally identifiable information, although you may request the reporter voluntarily provide contact information.*

*This is also a good place to pledge your agency to be as transparent as possible about what steps you are taking during the remediation process, as well as set expectations for when the reporter can anticipate acknowledgement of their report.*

*Information submitted under this policy will be used for defensive purposes only – to mitigate or remediate vulnerabilities.*

**We accept vulnerability reports at this form or via** [**security@agency.gov**](mailto:security@agency.gov). Reports may be submitted anonymously.

We will acknowledge receipt of your report within 3 business days.

We do not support PGP-encrypted emails at this time. For particularly sensitive information, submit through our HTTPS web form.

*Make sure that any web form you use has a strong HTTPS configuration. Reporters who are concerned about the sensitivity of their report may take steps to verify the HTTPS configuration first, and could be discouraged or alarmed if weak or compromised protocols or ciphers are in use.*

## What we would like to see from you

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

* 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.

## 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.

# Document change history

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Description** |
| 1.0 | *Month Day, Year* | First issuance. |