Appendix E - Disclosure Policy Templates

CERT Vulnerability Disclosure Policy Templates

In recent years the CERT/CC has advised a number of organizations on their vulnerability disclosure policies. In the interest of helping others develop or improve their own policies, we've collected policy items from a variety of vulnerability disclosure policies including our own, generalized them, organized them by topic, and put them into a git repository. The policy templates in this repository are meant to be remixed and adapted for different organizations and contexts. It is unlikely that any single organization would choose to adopt all of these items wholesale without some modification.

https://github.com/CERTCC/vulnerability_disclosure_policy_templates

NTIA Early Stage Template

The NTIA Early Stage Template focuses on vulnerability disclosure policy development in safety-critical industries, in which the potential for harm directly impacts public safety or causes physical damage (e.g., automobiles or medical devices), but the lessons are easily adaptable by any organization that builds or maintains its own software or systems. A discussion of issues and template policy is included.

https://www.ntia.doc.gov/files/ntia/publications/ntia_vuln_disclosure_early_stage_template.pdf

Disclose.io

> *disclose.io is a cross-industry, vendor-agnostic standardization project for* safe harbor† *best practices to enable good-faith security research.*

Main web site: https://disclose.io/

Github repository with policy templates: https://github.com/disclose/disclose

Open Source Vulnerability Disclosure Framework

BugCrowd and CipherLaw created the Open Source Vulnerability Disclosure Framework, offered under a Creative Commons Attribution 4.0 International License. The framework "is designed to quickly and smoothly prepare your organization to work with the independent security researcher community while reducing the legal risks to researchers and companies." In addition to a policy template "written with both simplicity and legal completeness in mind," a guidance document is provided for setting up a vulnerability disclosure program.

https://github.com/bugcrowd/disclosure-policy

Security.txt

security.txt: A proposed standard which allows websites to define security policies.

https://securitytxt.org/ and IETF draft https://tools.ietf.org/html/draft-foudil-securitytxt-08

U.S. GSA Vulnerability Disclosure Policy

The United States General Services Administration (GSA)'s Technology Transformation Service (TTS) provides its vulnerability disclosure policy as a public domain resource.

https://github.com/18F/vulnerability-disclosure-policy

ENISA Good Practice Guide on Vulnerability Disclosure

The Good Practice Guide on Vulnerability Disclosure from European Union Agency for Network and Information Security (ENISA) includes an annotated vulnerability disclosure policy template as an Annex.

https://www.enisa.europa.eu/publications/vulnerability-disclosure/at_download/fullReport

US Department of Justice Framework for a Vulnerability Disclosure Program for Online Systems

The United States Department of Justice (DoJ) has published a white paper containing guidance aimed at developing vulnerability disclosure programs for online systems and services. This report makes a point to distinguish online systems and services from "third-party vulnerability disclosure and hands-on—rather than remote—examination of software, devices, or hardware" because of potentially distinct legal issues that may arise.

https://www.justice.gov/criminal-ccips/page/file/983996/download

The aforementioned report is one of many related white papers provided by the DoJ's Computer Crime and Intellectual Property section.

https://www.justice.gov/criminal-ccips/ccips-documents-and-reports

Where to Look for More

Numerous organizations have already posted their vulnerability disclosure policies. A wide variety of these policies can be found by searching the web for "vulnerability disclosure policy," or "vulnerability disclosure program," or by browsing third-party vulnerability disclosure (e.g., bug bounty) service providers' hosted programs.