Cybersecurity
Policy Templates

CRF SANS

# Software Development Vulnerability Management Policy

*(Last Updated April 2025)*

## Purpose

Our Software Development Vulnerability Mangement Policy aims to establish standards for systematically examining software source code, focusing on identifying and rectifying potential security vulnerabilities, code inefficiencies, and deviations from established coding standards. This policy aims to enhance our software products' security, performance, and maintainability, thereby minimizing the risks associated with insecure coding practices and software defects. Through implementing this policy, we commit to developing secure, high-quality software that aligns with industry best practices, regulatory compliance standards, and the expectations of our stakeholders while upholding the integrity, confidentiality, and availability of our organizational digital assets.

## Scope

The Software Development Vulnerability Management Policy applies to all software code developed or utilized within our organization, including in-house development, third-party applications, and open-source software. This policy covers the analysis of code for security vulnerabilities, coding errors, and adherence to coding standards and best practices. It applies to all software development teams, software architects, programmers, and individuals responsible for reviewing and maintaining software code. The policy outlines the procedures, tools, and methodologies for code analysis, including static analysis, dynamic analysis, and manual code reviews. Compliance with this policy is mandatory to identify and mitigate potential security risks and vulnerabilities in software code. Any exceptions or deviations from this policy must be approved by the designated authority responsible for software code analysis and security.

## Safeguards

To achieve the organization's overall mission, and the purpose of this cybersecurity policy, the organization shall:

SDV-01 Maintain an issue-tracking system for each cybersecurity vulnerability identified in the organization's custom software applications.

SDV-02 Ensure that the organization's issue-tracking system tracks cybersecurity vulnerabilities identified in its custom software applications and tracks the criticality of each custom software application to assist the organization with threat modeling.

SDV-03 Ensure that the organization's issue-tracking system tracks cybersecurity vulnerabilities identified in the organization's custom software application, calculating the criticality of each vulnerability identified to assist the organization with threat modeling.

SDV-04 Maintain a software application code vulnerability scanner to scan each organization's custom software application for cybersecurity vulnerabilities.

SDV-05 Ensure that each of the organization's software application development teams is utilizing its software application code vulnerability scanner to scan each of their custom software applications.

SDV-06 Ensure that each cybersecurity vulnerability identified by the software application code vulnerability scanner is reported to the organization's issue-tracking system.

SDV-07 Maintain an approved inventory of each software library and third-party module used by the organization's software application development teams.

SDV-08 Ensure that each of the approved software libraries and third-party modules used by the organization's software application development teams is still maintained and supported by its creator.

SDV-09 Ensure that each of the approved software libraries and third-party modules used by the organization's software application development teams is kept up to date with the latest cybersecurity-related updates.

SDV-10 Ensure that each of the approved software libraries and third-party modules used by the organization's software application development teams is scanned regularly for cybersecurity vulnerabilities.

SDV-11 Ensure that each cybersecurity vulnerability identified by the software library and third-party module scanner is reported to the organization's issue-tracking system.

SDV-12 Maintain a process for individuals inside or outside the organization to report software application vulnerabilities to the organization's issue-tracking system.

SDV-13 Maintain documented Service Level Agreements (SLAs) that define the organization's timing targets for mitigating cybersecurity vulnerabilities discovered in the organization's custom software applications.

SDV-14 Ensure that each of the cybersecurity vulnerabilities tracked by the organization's issue tracking system are remediated in accordance with the organization's documented Service Level Agreements (SLAs).

SDV-15 Ensure that each cybersecurity vulnerability tracked by the organization's issue-tracking system is reported to the appropriate stakeholders regularly.

## Policy Sanctions

Non-compliance with this policy may result in disciplinary action in line with our corporation's human resources procedures. Consequences may range from mandatory refresher training and written warnings to temporary suspension of remote access privileges and, in severe cases, termination of employment or contractual obligations. Individuals could be subject to legal consequences under applicable laws if violations involve illegal activities. These sanctions emphasize the critical importance of cybersecurity, the individual's role in protecting our digital assets, and the potential risks associated with policy violations. Enforcement will be consistent and impartial, with the severity of the action corresponding directly to the seriousness of the breach.