Static Application Security Testing (SAST) Policy

AI Security Policy Framework

The organization adopts a risk-based SAST program aligned with NIST CSF and ISO 27001 to continuously detect code-level weaknesses. Current findings are limited to a single low-severity issue, indicating an overall healthy code security posture while...

Generated: November 13, 2025

Static Application Security Testing (SAST) Policy

Policy Metadata

Policy ID	POL-SAST-2025-001
Status	Active
Created Date	2025-11-05T00:00:00
Last Updated	2025-11-05T00:00:00
Author	Security Policy Generator

Executive Summary

The organization adopts a risk-based SAST program aligned with NIST CSF and ISO 27001 to continuously detect code-level weaknesses. Current findings are limited to a single low-severity issue, indicating an overall healthy code security posture while highlighting the need for ongoing review of unknown findings.

Policy Statement

Purpose

To establish standards for identifying and remediating source code vulnerabilities through static analysis.

Description

This policy defines requirements for SAST implementation, vulnerability management, and secure code development practices across the organization.

Applicability

All development teams and applications that contain custom source code, including micro-services, libraries, and scripts.

Enforcement

Mandatory SAST scans must be integrated into every CI/CD pipeline with defined quality gates; builds failing the gate are blocked from promotion.

Exceptions

Legacy applications may request temporary exemptions through the Security Review Board, subject to a documented risk acceptance and remediation timeline.

Objectives

1. Integrate automated static analysis into every code commit and build process.
2. Ensure identified vulnerabilities are triaged, prioritized, and remediated within defined timeframes.
3. Maintain compliance with NIST CSF Protect function and ISO 27001 A.14 System Development lifecycle controls.

Risk Assessment

Risk Metric	Value
Overall Risk Level	Low
Critical Risks	0
High Risks	0
Medium Risks	0
Low Risks	1
Likelihood	Low

Security Controls

SC-001: Input Validation Framework

Implement a centralized input validation library that enforces whitelist-based checks for all external data.

- Select a vetted validation library (e.g., OWASP ESAPI).
- Integrate the library into all new code modules.
- Refactor existing modules to use the library within 90 days.
- Document validation rules per data source in the code repository.

SC-002: Automated SAST Integration

Configure CI/CD pipelines to run approved SAST tools on every pull request and nightly builds.

- Deploy SAST tool (e.g., SonarQube, Checkmarx) on the build server.
- Create pipeline step that fails the build if findings exceed the defined threshold.
- Generate a SARIF report and store it in the artifact repository.
- Notify the development team via Slack/Email on each scan result.

SC-003: Vulnerability Triage and Response Process

Establish a formal process to triage SAST findings, assign remediation owners, and track closure.

- Log each finding in the ticketing system with severity tags.
- Assign tickets to the responsible component owner within 1 business day.
- Review tickets in weekly security stand-ups.

- Close tickets only after successful re-scan and peer review.

Remediation Actions

P3: Review and fix unknown security report analysis finding

Owner: Backend Development Team | Timeline: Within 14 days

Affected Assets:

- Application code base (global scope)
- CI/CD pipeline configuration

Success Criteria: The unknown finding is either resolved or documented with a risk acceptance; subsequent SAST scan shows no recurrence of the same issue.

Compliance Mapping

Framework	Controls
NIST CSF	• PR.DS-5 • PR.IP-1 • DE.CM-4
ISO 27001	• A.14.2.1 • A.14.2.5 • A.12.6.1

Monitoring Requirements

- Automated SAST scans on every code commit (CI) and nightly full scans (CD).
- Weekly reporting of new findings to the Security Steering Committee.
- Quarterly security code reviews by peer developers and the Application Security Team.

Review Schedule

Quarterly policy review and annual audit