# Reusable Component Library System Security Plan

# NIST SP 800-53 Revision 4

## SI: System and Information Integrity

### SI-1: System And Information Integrity Policy And Procedures

The organization:  
 a. Develops, documents, and disseminates to [Assignment: organization-defined  
personnel or roles]:  
 1. A system and information integrity policy that addresses purpose, scope,  
roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and  
 2. Procedures to facilitate the implementation of the system and information  
integrity policy and associated system and information integrity controls; and  
 b. Reviews and updates the current:  
 1. System and information integrity policy [Assignment: organization-defined  
frequency]; and  
 2. System and information integrity procedures [Assignment: organization-defined  
frequency].

**Status:** Complete

##### CivicActions

CivicActions has developed, documented and disseminated to personnel a system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the policy and associated controls. This information is maintained in the CivicActions System and Information Integrity (SI) Policy document that can be found in the CivicActions GitHub repository at <https://github.com/CivicActions/compliance-docs/>.

### SI-2: Flaw Remediation

The organization:  
 a. Identifies, reports, and corrects information system flaws;  
 b. Tests software and firmware updates related to flaw remediation for effectiveness  
and potential side effects before installation;  
 c. Installs security-relevant software and firmware updates within [Assignment:  
organization-defined time period] of the release of the updates; and  
 d. Incorporates flaw remediation into the organizational configuration management  
process.

**Status:** Complete

#### a

##### CivicActions

Identification of information system security flaws are detected as early as possible by the following methods:

* Vulnerability scans, as described in RA-5.
* Log analysis from monitoring described in SI-4.
* Service flaw notifications (CVEs, etc.) are received by the CivicActions Security Office and passed on to CivicActions Operations staff when relevant.

Any security issues found are ticketed through JIRA and/or the Git issue queue. CivicActions Operations staff prioritizes high findings. Changes made to correct the information system as a result of the system flaws are scheduled and coordinated through the CCB Change Request Process and appropriate approvals required from the CCB as implemented in CM-3.

#### b

##### CivicActions

CivicActions testing of the system as a result of security flaw remediation is done through a development environment through the use of internal software and automated testing that ensures the system is working as intended. When a change is made by a developer, testing though a peer review is conducted as part of the Change Request process to ensure the correct analysis is completed. Then the changed code is tested in an automatic test environment as described in the Configuration Management Plan (CMP). Tracking of the testing is documented in JIRA and/or the Git issue queue.

#### c

##### CivicActions

CivicActions security-software updates are tested prior to implementation on production. The CivicActions Security framework for installation requires updates to be made within 30 days for high vulnerabilities, 90 days for moderate vulnerabilities, and 240 for low vulnerabilities. An issue ticket is created to track any updates made to the system.

#### d

##### CivicActions

Flaw remediation is part of the CivicActions configuration management process. Any security issues found are ticketed through JIRA or the Git issue queue. The CivicActions Security Office prioritizes the high findings within the application. Changes made to correct the system as a result of the system flaws are scheduled and coordinated through the CCB Change Request Process and appropriate approvals required from the CCB Chair as implemented in CM-3.

### SI-3: Malicious Code Protection

The organization:  
 a. Employs malicious code protection mechanisms at information system entry  
and exit points to detect and eradicate malicious code;  
 b. Updates malicious code protection mechanisms whenever new releases are available  
in accordance with organizational configuration management policy and procedures;  
 c. Configures malicious code protection mechanisms to:  
 1. Perform periodic scans of the information system [Assignment: organization-defined  
frequency] and real-time scans of files from external sources at [Selection (one or more); endpoint; network entry/exit points] as the files are downloaded, opened, or executed in accordance with organizational security policy; and  
 2. [Selection (one or more): block malicious code; quarantine malicious code; send  
alert to administrator; [Assignment: organization-defined action]] in response to malicious code detection; and  
 d. Addresses the receipt of false positives during malicious code detection  
and eradication and the resulting potential impact on the availability of the information system.

**Status:** Complete

#### a

##### CivicActions

Virus scans are performed by ClamAV, a server-hosted tool protecting the application from Trojans, Viruses and other malicious cyber-threats. Real-time scans are conducted whenever files are uploaded from any external source and malicious code is blocked or quarantined when detected. All file-based traffic traversing the server is sanitized before being delivered. All input form text is validated and sanitized.

#### b

##### CivicActions

Anti-virus definitions and malicious code protection mechanisms are configured and updated automatically on a nightly basis.

#### c

##### CivicActions

CivicActions Operations staff receives information system security alerts, advisories, and notifications in response to malicious code detection. These messages are sent to group email distribution lists to ensure all members of the team receive the proper information in a timely manner.

#### d

##### CivicActions

False positives during malicious code detection and eradication are dealt with on a case by case basis. Potential impacts on the availability of the information system are detailed in a false positive report depending on if the report is for the OS, database or web application.

### SI-4: Information System Monitoring

The organization:  
 a. Monitors the information system to detect:  
 1. Attacks and indicators of potential attacks in accordance with [Assignment:  
organization-defined monitoring objectives]; and  
 2. Unauthorized local, network, and remote connections;  
 b. Identifies unauthorized use of the information system through [Assignment:  
organization-defined techniques and methods];  
 c. Deploys monitoring devices:  
 1. Strategically within the information system to collect organization-determined  
essential information; and  
 2. At ad hoc locations within the system to track specific types of transactions  
of interest to the organization;  
 d. Protects information obtained from intrusion-monitoring tools from unauthorized  
access, modification, and deletion;  
 e. Heightens the level of information system monitoring activity whenever there  
is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;  
 f. Obtains legal opinion with regard to information system monitoring activities  
in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and  
 g. Provides [Assignment: organization-defined information system monitoring  
information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].

**Status:** Complete

#### a

##### CivicActions

CivicActions systems use a collection of monitoring systems, including:

* ClamAV - provides signature-based malware detection/quarantine
* OSSEC host-based intrusion detection system (HIDS)
* AIDE Advanced Intrusion Detection Environment (IDS))
* fail2ban, an intrusion prevention system (IPS) framework
* SELinux - a Mandatory Access Control (MAC) IPS
* auditd - a secure system audit daemon
* CloudWatch - AWS monitoring and measurement system
* StatusCake - website monitoring tool
* OpsGenie - a slack/email/text/phone incident escalation tool

#### b

##### CivicActions

Logs from the systems described in SI-4(a) are sent to the CivicActions SIEM tool for analysis. These logs can identify unauthorized use of the information system.

#### c

##### CivicActions

Monitoring and log collection occur throughout the system.

#### d

##### CivicActions

The Configuration Management process, remote log gathering, and SELinux MAC protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.

#### e

##### CivicActions

In the event of a performance score lower than CivicActions standards, a notification is sent to the CivicActions Security Office. CivicActions subscribes to security mailing lists in the event the monitoring activity is required based on law enforcement information, intelligence information, or other credible sources of information.

#### f

##### CivicActions

Internal legal counsel is utilized as required when system notifications indicate such action based on user and/or malicious activity. Legal counsel is engaged for any actions that may necessitate increased user monitoring or evidence/forensic actions.

#### g

##### CivicActions

System alerts generated by CivicActions internal monitors (StatusCake, OSSEC, ClamAV, others) are sent to the Incident Response team via OpsGenie.

### SI-5: Security Alerts, Advisories, And Directives

The organization:  
 a. Receives information system security alerts, advisories, and directives  
from [Assignment: organization-defined external organizations] on an ongoing basis;  
 b. Generates internal security alerts, advisories, and directives as deemed  
necessary;  
 c. Disseminates security alerts, advisories, and directives to: [Selection  
(one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; and  
 d. Implements security directives in accordance with established time frames,  
or notifies the issuing organization of the degree of noncompliance.

**Status:** Complete

#### a

##### CivicActions

The CivicActions Security Office and Operations staff receive the following security alerts, advisories, and directives on an ongoing basis:

* Mailing lists relevant to web application security
* US-CERT
* Technical Cyber Security Alerts
* Drupal Security Advisories

#### b

##### CivicActions

CivicActions utilizes StatusCake for front line monitoring for real time system status and events of the application. StatusCake can feed to the OpsGenie incident escalation system.

#### c

##### CivicActions

The CivicActions Security Office disseminates security alerts, advisories, and directives to all CivicActions internal personnel and client personnel as directed.

#### d

##### CivicActions

The CivicActions Security Office is responsible for ensuring the dissemination and implementation of relevant security alerts and advisories.

### SI-12: Information Handling And Retention

The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

**Status:** Complete

##### CivicActions

The CivicActions organization retains all information, system-related information, incident-related information, and system output in accordance with customers’ requirements retention periods and other NIST guidance and standards, Federal policies, procedures, federal laws, and executive orders. Audit records are retained for 365 days.