# Reusable Component Library System Security Plan

# NIST SP 800-53 Revision 4

## PL: Planning

### PL-1: Security Planning Policy And Procedures

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

##### AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud Service Provider dated 1 May 2013.

##### CivicActions

CivicActions has developed, documented and disseminated to personnel a system planning 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 Planning (PL) Policy and Procedure document that can be found in the CivicActions Github repository at <https://github.com/CivicActions/compliance-docs/>.

### PL-2: System Security Plan

The organization: a. Develops a security plan for the information system that: 1. Is consistent with the organization�s enterprise architecture; 2. Explicitly defines the authorization boundary for the system; 3. Describes the operational context of the information system in terms of missions and business processes; 4. Provides the security categorization of the information system including supporting rationale; 5. Describes the operational environment for the information system and relationships with or connections to other information systems; 6. Provides an overview of the security requirements for the system; 7. Identifies any relevant overlays, if applicable; 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and 9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Distributes copies of the security plan and communicates subsequent changes to the plan to [Assignment: organization-defined personnel or roles]; c. Reviews the security plan for the information system [Assignment: organization-defined frequency]; d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and e. Protects the security plan from unauthorized disclosure and modification.

##### AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: AWS system security plan.

#### a

##### CivicActions

CivicActions has developed this system security plan (SSP) for the information system as part of compliance with NIST 800-53 and FIPS 199. The SSP defines the security categorization, system boundary, and security requirements and controls meeting the requirements of the NIST Risk Management Framework (RMF). Specifically the SSP: 1. Is consistent with the organization’s enterprise architecture 2. Explicitly defines the authorization boundary for the system 3. Describes the operational context of the information system in terms of missions and business processes 4. Provides the security categorization of the information system including supporting rationale 5. Describes the operational environment for the information system and relationships with or connections to other information systems 6. Provides an overview of the security requirements for the system 7. Identifies any relevant overlays, if applicable 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions 9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation

#### b

##### CivicActions

The SSP is reviewed and approved by the authorizing official prior to plan implementation. A copy of the SSP is provided to authorized CivicActions and assessing personnel including the System Owner, Authorizing Official, Information System Security Officer, System/Network Administrator, and CivicActions’ Operations staff. The SSP is maintained by CivicActions’ Security Office.

#### c

##### CivicActions

The SSP is reviewed at least annually by the System Owner and CivicActions’ Operations staff in collaboration with CivicActions’ Security Office.

#### d

##### CivicActions

CivicActions’ Operations staff in collaboration with CivicActions’ Security Office updates the system description and control descriptions within the SSP as needed to verify the SSP is an accurate description of the system.

#### e

##### CivicActions

The SSP is currently available to authorized users on GitLab. Per the Acceptable Use Policy, all entities granted access to CivicActions information assets are required to complete a non-disclosure agreement (NDA) to uphold information confidentiality. GitLab provides the configuration management capabilities for the SSP to be protected from unauthorized disclosure and modification.

### PL-4: Rules Of Behavior

The organization: a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; b. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system; c. Reviews and updates the rules of behavior [Assignment: organization-defined frequency]; and d. Requires individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.

#### a

##### CivicActions

CivicActions has created and made readily available to individuals requiring access to the information system the rules that describe their responsibilities and expected behavior with regard to information and information system usage. These rules, defined as the Acceptable Use Policy, are included in the CivicActions Security Policy accessible here: <https://civicactions-handbook.readthedocs.io/en/latest/03-policies/security/#acceptable-use-policy> which has also been uploaded to CSAM as ‘Appendix J1 - System Rules of Behavior - Privileged User’ (CivicActions Security Policy 20190226.docx).

#### b

##### CivicActions

CivicActions HR receives a signed acknowledgment from all employees, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system. The text of the electronically signed (via DocuSign) acknowledgment document has been uploaded to CSAM as artifact: ‘CivicActions Security Policy Acknowledgement.docx’

#### c

##### CivicActions

CivicActions reviews the CivicActions Security Policy at least annually and updates as required.

#### d

##### CivicActions

CivicActions requires individuals who have signed a previous version of the CivicActions Security Policy to read and re-sign when any part of it, including the Acceptable Use Policy/Rules of Behavior, is revised/updated.