# 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].

**Status:** Complete

##### 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/>.

##### Project

This is Agency common control. More data about implementation can be obtained from the Agency common control catalog.

The Project developed its security policy planning and procedures based on None, guidance from NIST, the Office of Management and Budget and industry best practices. Security policies and procedures are formally documented within the Project SSP, which provides the roles and responsibilities as it pertains to security planning. It provides guidance on all aspects of security for the protection of Project information technology resources. It defines responsibilities for the implementation and oversight of the guidance contained herein. The plan was last updated in December, 2015.

### 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.

**Status:** Complete

##### 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.

##### Project

The System Security Plan (SSP) was developed and implemented for Project system in accordance with None, NIST SP 800-18 and NIST SP 800-37. The SSP includes a description of the management, operational, and technical controls in place or planned for the application. The SSP is included as a key document in an application’s C&A package and is reviewed and approved by designated officials. The SSP identifies the system owner and responsible parties for managing system access and the overall security of the system. The Chief Information Security Officer reviews and approves the SSP. The SSP will be reviewed at least annually and updated to account for any changes to the Project system and to address any changes in security controls.

#### 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 the CivicActions Operations staff. The SSP is maintained by the CivicActions Security Office.

#### c

##### CivicActions

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

#### d

##### CivicActions

The CivicActions Operations staff in collaboration with the 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.

**Status:** Complete

#### 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).’

##### Project

Project has created and made readily available to individuals requiring access to the information system the rules that describes their responsibilities and expected behavior with regard to information and information system usage. These rules are captured in ‘Appendix J2 - System Rules of Behavior - General User’ (ProjectSystemRoB2019-template.docx).

Project has reviewed and accepted as a superset alternative the CivicActions Acceptable Use Policy.

#### 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’’

##### Project

The Project System Owner receives a signed acknowledgment from such individuals that are not CivicActions 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.

#### c

##### CivicActions

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

##### Project

Project reviews the Rules of Behavior at least annually and updates it 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.

##### Project

Project 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.