# Reusable Component Library System Security Plan

# NIST SP 800-53 Revision 4

## CM: Configuration Management

### CM-1: Configuration Management Policy And Procedures

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

##### AWS

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

##### CivicActions

CivicActions has developed, documented and disseminated to personnel a configuration management 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 Configuration Management (CM) Policy. This document can be found in the CivicActions Compliance Docs GitHub repository at <https://github.com/CivicActions/compliance-docs>. Configuration changes are overseen by the Change Control Board (CCB) consisting of the System Owner, Project Manager, CivicActions Operations staff and the engineering team.

### CM-2: Baseline Configuration

The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

##### AWS

Hardware Baselines All hardware is maintained by AWS Cloud. The system therefore inherits hardware configuration aspects of this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: baseline configuration.

##### CivicActions

A current baseline configuration is always available - stored as a tag in the Git repository - such that the site can be regenerated or rolled back should unauthorized or failing changes be applied.

##### Drupal

The baseline configuration is maintained in Git and described in the Configuration Management Plan, which describes the change workflow and software configuration. In the context of Security Configuration Management, the baseline configuration is a collection of formally approved configuration state(s) of one or more configuration items (“features”) that compose the system. The baseline configuration is used to restore and serves as the basis against which the next change or set of changes to the system is made. The features for the system are maintained in the website’s source code, which is managed in Git, a source code version control system. Once the source code is updated, Git maintains the new version of staged code once committed in the Git repository as the new baseline. All code prior to it being staged is documented, tested and approved by CivicActions Development, which is described in control SA-3. The production environment is configured to take database snapshots daily.

### CM-2 (1): Reviews And Updates

The organization reviews and updates the baseline configuration of the information system: (1)(a). [Assignment: organization-defined frequency]; (1)(b). When required due to [Assignment organization-defined circumstances]; and (1)(c). As an integral part of information system component installations and upgrades.

##### Drupal

CivicActions reviews and updates baseline configurations for the system at least annually, when requested by the System Owner or required by law, and as an integral part of information system component installations, upgrades, and maintenance. A review of the CM baselines for the system is conducted and approved by CivicActions Development. Any changes made to the production environment are approved prior to deployment by the CCB or agile scrum process. Changes that may require updates to the baseline configuration for the application include: • Significant upgrades or changes to applications or database software • Security assessment findings • Changes in internal/external security requirements • A new security threat, incident, or event

### CM-2 (2): Automation Support For Accuracy / Currency

The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

##### Drupal

Drupal configuration settings use automated mechanisms to automate code deployment and baseline settings changes. The website’s baseline configuration may be reapplied to the site at any time by manually retriggering a tagged code deployment. The source code, which contains the site’s baseline configuration, is managed using Git, a source code version control system. Git is used to track source code which allows administrators to easily deploy and roll back changes on production hosting environments. The Features module is used to export configuration settings from the website’s MySQL database and stores them as code so that the configuration settings can be managed within the Git source code version control system.

### CM-2 (3): Retention Of Previous Configurations

The organization retains [Assignment: organization-defined previous versions of baseline configurations of the information system] to support rollback.

##### Drupal

Previous baseline configurations are retained in Git, which implements unlimited revision control. Each version of the codebase is given a unique tag when it is deployed to production. When new features are ready for deployment to production, the new code release is given a new tag. This makes it possible to roll back to a previous version of the baseline configuration if needed by redeploying the older release tag.

### CM-3: Configuration Change Control

The organization: a. Determines the types of changes to the information system that are configuration-controlled; b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; c. Documents configuration change decisions associated with the information system; d. Implements approved configuration-controlled changes to the information system; e. Retains records of configuration-controlled changes to the information system for [Assignment: organization-defined time period]; f. Audits and reviews activities associated with configuration-controlled changes to the information system; and g. Coordinates and provides oversight for configuration change control activities through [Assignment: organization-defined configuration change control element (e.g., committee, board)] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]].

##### CivicActions

In accordance with the Configuration Management Plan and control SA-3, CivicActions manages changes to the baseline configuration of the application through an agile scrum-based process. Examples of the types of changes that may be introduced through a code release include the following, ordered by increasing level of possible security risk: 1. Minor application code changes 2. New software releases for Drupal core, contributed Drupal modules, or other software components that are supplied by outside open-source vendors 3. Significant software enhancement 4. Major application modification The CCB meets bi-weekly during the sprint planning and backlog grooming meetings. In addition, the System Owner or Project Manager may convene the CCB in an emergency session to address time-critical topics as deemed necessary.

#### b

##### CivicActions

In accordance with the Configuration Management Plan, CivicActions performs security impact analysis of all planned code releases. The level of impact is assessed by CivicActions Operations staff in collaboration with CivicActions’ Security Office before the planned code updates are presented at the sprint planning meeting for approval. Significant software enhancements and major application modifications require approval from the Tech Lead of the Development team. Once a code release is considered ready for deployment, a Security Review is done before scheduling deployment of the code release to production, in accordance with the Agile-based System Development Life Cycle methodology described in SA-3.

#### c

##### CivicActions

Configuration changes follow the CivicActions sprint planning process. The changes themselves are documented within a JIRA ticket tracking system. The JIRA ticket has an approval step built into the ticketing workflow that is required before the implementation phase. The CCB (agile sprint planning process) is responsible for reviewing the change and either approving or rejecting the proposal. These workflow changes are captured within an audit log in the ticket and are available to anyone viewing the ticket.

#### d

##### CivicActions

See part b). Configuration changes are captured within tickets in the CivicActions ticketing system. Each CR follows a specific workflow within the ticketing system that follows our process: 1. Open (Backlog) 2. To Do 3. In Progress 4. QA 5. Signoff All CRs must be approved before they are applied to the information system.

#### e

##### CivicActions

All changes are logged and retained for a minimum of three years in the ticketing system. The Change Request (CR) tickets contain a detailed record of the steps taken to implement the change, as well as dates of approval and implementation.

#### f

##### CivicActions

All changes are logged and retained for a minimum of three years in the ticketing system. The Change Request (CR) tickets contain a detailed record of the steps taken to implement the change, as well as dates of approval and implementation.

#### g

##### CivicActions

The CivicActions Change Control Board (or agile Sprint Planning team) meets bi-weekly, or when operational or security imperatives require, to address requested changes to the application.

### CM-3 (2): Test / Validate / Document Changes

The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

##### CivicActions

CivicActions tests and validates changes to the system before implementing the changes in production. Changes are documented as code and comments in the git source code version control system. Any changes made to system are first captured in a separate development branch of git that is used to create a pull request, which is reviewed for quality and security control before being merged into the master branch of the repository.

### CM-4: Security Impact Analysis

The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

##### CivicActions

Security impact analysis is conducted and documented within the Change Request (CR) process described in CM-3(b). All proposed configuration-controlled changes to the application are tested first in a sandboxed development environment before being pushed to a staging environment to be tested by another developer and by the Engineering team prior to final approval from CCB to move changes to the production environment.

### CM-5: Access Restrictions For Change

The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

##### AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: physical and logical access restrictions to server instances. Development and staging environments are logged by default as part of the AWS Cloud system.

##### CivicActions

CivicActions restricts system logical access to only those internal personnel assigned to work on the application. Logical access is governed by the implementation described in AC-3 and the concept of least privilege requirements implemented by AC-6. All-access to server environments is via an encrypted SSH session with public-key authentication, and all server access is logged.

### CM-5 (1): Automated Access Enforcement / Auditing

The information system enforces access restrictions and supports auditing of the enforcement actions.

##### AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: automated access enforcement / access.

##### Drupal

Access enforcement is monitored within Drupal, which records an entry in the Drupal Watchdog log for every successful or failed login attempt to the system. Each successful login or logout event is logged with an entry that includes the username of the account being used. Access to the server environments is via encrypted SSH sessions with public-key authentication, and all server access is logged. Specific implementation of auditing events are captured in AU-2. The same access control procedures and need-to-know and accountability principles are enforced for all systems storing baseline configuration policies.

### CM-5 (5): Limit Production / Operational Privileges

The organization: (5)(a). Limits privileges to change information system components and system-related information within a production or operational environment; and (5)(b). Reviews and reevaluates privileges [Assignment: organization-defined frequency].

#### a

##### Drupal

Configuration changes that do not entail software code changes can only be performed by CivicActions internal administrators with privileges implemented by access enforcement (AC-3) and least privilege (AC-6).

#### b

##### CivicActions

CivicActions’ internal administrator user access rights are reviewed at least quarterly by CivicActions’ Security Office, which is responsible for approving all user account assignments to CivicActions developers.

### CM-6: Configuration Settings

The organization: a. Establishes and documents configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves any deviations from established configuration settings for [Assignment: organization-defined information system components] based on [Assignment: organization-defined operational requirements]; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

##### AWS

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

##### Drupal

CivicActions configuration settings for Drupal are guided by the Drupal Security Coding Standards <https://www.drupal.org/docs/develop/security> for the security configuration management processes and tools.

#### b

##### CivicActions

CivicActions developers follow security best practices according to the guidelines set by CivicActions’ Security Office.

#### d

##### CivicActions

All changes to the configuration settings are logged in the Git source code version control system, which records the identity of the developer who committed each change. Version control is enforced, with previous tagged code releases kept for rollback purposes.

### CM-7: Least Functionality

The organization: a. Configures the information system to provide only essential capabilities; and b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services].

##### AWS

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

### CM-8: Information System Component Inventory

The organization: a. Develops and documents an inventory of information system components that: 1. Accurately reflects the current information system; 2. Includes all components within the authorization boundary of the information system; 3. Is at the level of granularity deemed necessary for tracking and reporting; and 4. Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]; and b. Reviews and updates the information system component inventory [Assignment: organization-defined frequency].

##### AWS

The system inherits the platform software components of this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: information system component inventory.

##### Drupal

The software inventory for the application is maintained in the codebase stored CivicActions’ Git source code version control system. It consists of the following components: • The Drupal open source web content management system • Drupal add-on modules, themes, and libraries available from the Drupal.org website which extend Drupal core • Custom code written by CivicActions’ developers The inventory is reviewed monthly by CivicActions Product Engineering teams in accordance with the Configuration Management Plan. Website content is backed up daily using CPM snapshots. This allows CivicActions to build an inventory of the system on demand.

### CM-8 (1): Updates During Installations / Removals

The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

##### AWS

Website content is backed up daily by the AWS Managed Cloud hosting system, which is configured to take daily database snapshots The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: components inventory updates.

##### CivicActions

CivicActions stores all software code in a git source version control repository which is updated for all component installations, removals, and information system updates. This allows CivicActions to build an inventory of the system on demand.

### CM-10: Software Usage Restrictions

The organization: a. Uses software and associated documentation in accordance with contract agreements and copyright laws; b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

##### AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud Service Providers dated 1 May 2013 for the following: software usage restrictions.

##### Drupal

Drupal is hosted on a LAMP platform (Linux, Apache, MySQL, and PHP). These are all compatible with the Free Software Foundation’s General Public License (GPL) version 2 or later and are freely available for use under copyright law.

### CM-11: User-Installed Software

The organization: a. Establishes [Assignment: organization-defined policies] governing the installation of software by users; b. Enforces software installation policies through [Assignment: organization-defined methods]; and c. Monitors policy compliance at [Assignment: organization-defined frequency].

#### a

##### AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud Service Providers dated 1 May 2013 for the following: governing user installed software.

##### CivicActions

All software installed in the system environment must be first approved via the CCB resulting in a Change Request (CR) being initiated and executed. Software installation on the computing nodes within the authorization boundary is restricted to administrators. All CivicActions internal administrators are informed of this during their initial training and as part of the rules of behavior document.

#### b

##### AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud Service Providers dated 1 May 2013 for the following: enforcing software installation policies.

##### CivicActions

CivicActions enforces software installation policies through required acknowledgment and sign-off on acceptable use policy by CivicActions personnel. CivicActions Development is responsible for enforcing compliance with the acceptable use policy.

#### c

##### AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud Service Providers dated 1 May 2013 for the following: monitoring compliance.

##### CivicActions

CivicActions monitors policy compliance continuously via the code release planning and quality control systems built into the System Development Life Cycle described in control SA-3.