# 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].

##### 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.

##### Project

The configuration management policy and procedures are formally documented in the Project Configuration Management Plan (CMP), which provides the roles and responsibilities as it pertains to physical and environmental protection. It defines responsibilities for the implementation and oversight of the guidance contained herein. Client reviews and updates the policy as necessary.

### 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 the AWS cloud. The system inherits hardware configuration aspects of this control from the FedRAMP Provisional ATO granted to AWS, 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.

##### Ilias

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.

##### Project

A CM process has been established and documented in the Project CMP. All updates are made in accordance with the procedures outlined in the CMP. The CM process establishes a baseline of hardware, software, firmware and documentation, as well as changes thereto, throughout the development and life cycle of the information system. CM ensures the control of the information system through its life cycle. It assures that additions, deletions, or changes made to the Project system do not unintentionally or unknowingly diminish security. If the change is major, the security of the system must be re-analyzed.

### 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.

##### Project

An Information Security Program is in place to ensure all security-centric impacts to the Project are properly analyzed and conducted by personnel with information security responsibilities (i.e., Project SSO, IT Security Officer, etc.). These individuals have the appropriate skills and technical expertise to analyze the changes to the Project and their associated security ramifications. In support of continuous monitoring and to ensure the Project system lifecycle is fully sustained, a risk assessment process, be it formal or informal, is performed when changes are occur. This ensures that Client Full Name understands the security impacts and can determine if additional security controls are required.

### 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.

#### a

##### Project

The Project is configured in compliance with the applicable baseline security standards. The Department and its technical support staff configure the security settings of all IT products to the most restrictive mode consistent with information system operational requirements. Project utilizes the NIST Special Publication 800-70 for guidance on configuration settings (checklists) for information technology products. When security setting checklist are not available from NIST for a particular device, good security engineering practices along with manufacture guidelines is used to develop the security settings. The CM Manager conducts configuration audits to ensure baseline compliance and documentation of hardware/software configurations throughout the system lifecycle.

#### b

##### CivicActions

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

##### Project

Configuration settings are implemented, monitored, and controlled in accordance with the organizational Configuration Management Plan for the security configuration management processes and tools.

#### c

##### Project

Currently, deviations do not exist for established configuration settings. In the event this changes, the following notes the process that will take place. The CivicActions CCB, identifies, approves, and documents exceptions to mandatory configuration settings for individual components within its cloud offering only when operationally necessary. All variances identified during the monthly and annual system testing scans that must be accepted for operational purposes are tracked.

#### 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].

#### a

##### AWS

In this architecture, only essential capabilities for a multi-tiered web service are configured. AWS Identity and Access Management (IAM) baseline Groups and Roles are configured to support restricted access to AWS resources by privileged users and non-person entities (Amazon EC2 systems operating with a role) authorized and assigned by the organization.

##### Project

Services are limited to provide only essential capabilities.

#### b

##### AWS

In this architecture, ports, protocols, and services are restricted to those that are required for a multi-tiered web service, via AWS security group rules.

##### Project

The Project maintains strict default deny policy with access controls at the firewall, and on individual systems. Inbound access across the system boundary is only allowed on ports 22 (ssh), 80 (http) and 443 (https), with an additional port, 25 (smtp) open on the mail server.

### 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].

##### Ilias

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 Ilias open-source web learning management system - Ilias add-on modules, themes, and libraries available from the Ilias.de website which extend Ilias 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.

#### a

##### AWS

AWS built-in features dynamically build and maintain an inventory of system components (infrastructure inventory)

1. AWS built-in features provide an accurate, real time inventory of all infrastructure system and network components within the customer account and provides a single view for granularity for tracking and reporting.
2. AWS built-in features provide an accurate, real time inventory of all infrastructure system and network components within the AWS account, and AWS CloudFormation creates a unique set of stack names, and associated resource names incorporate the stack name, for tracking components deployed by CloudFormation templates that align with an authorization boundary.
3. AWS built-in features provide a level of granularity for tracking and reporting on all infrastructure system and network components and configuration settings for those components.
4. AWS built-in features provide all available information about all infrastructure system and network components to achieve effective component accountability.

#### b

##### AWS

AWS built-in features provides a dynamically updated inventory of all infrastructure system and network components within the customer account. The AWS management console and AWS API calls support the capability for the organization to review the inventory.

### 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.

##### CivicActions

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.

##### Ilias

Ilias 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

##### 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

##### 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

##### 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.