# CONFIGURATION MANAGEMENT

## CM-01 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

Control description: <http://800-53.govready.com/control?id=CM-1>

Security control type: Hybrid

#### LINCS specific control or LINCS Responsibility

The configuration management policy and procedures are formally documented in the LINCS Technology 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. The Department reviews and updates the policy as necessary.

Additional information is contained within the Department of Education, Handbook forInformation Technology Security Configuration Management Planning Procedures (Handbook OCIO-11).

#### CivicActions Responsibility

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 and CivicActions Development.

#### Amazon Web Services (AWS) US-East/West control support

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

## CM-02 BASELINE CONFIGURATION

Control description: <http://800-53.govready.com/control?id=CM-2>

Security control type: Hybrid

#### LINCS specific control or LINCS Responsibility

A CM process has been established and documented in the LINCS Technology 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 LINCS Technology Project system do not unintentionally or unknowingly diminish security. If the change is major, the security of the system must be re-analyzed.

#### CivicActions Responsibility

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 specific control support

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.

#### Amazon Web Services (AWS) US-East/West control support

The system inherits server configuration aspects of this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: baseline configuration for IaaS components.

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.

Server Configuration

AWS maintains the baseline software configuration for the server components required to run the Drupal platform upon which the system is built.

## CM-02 (1) REVIEWS AND UPDATES

Control description: <http://800-53.govready.com/control?id=CM-2>

Security control type: Hybrid

#### Drupal specific control support

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.

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

### Part c)

#### Amazon Web Services (AWS) US-East/West control support

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

## CM-02 (2) AUTOMATION SUPPORT FOR ACCURACY / CURRENCY

Control description: <http://800-53.govready.com/control?id=CM-2>

Security control type: Hybrid

#### Drupal specific control support

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-02 (3) RETENTION OF PREVIOUS CONFIGURATIONS

Control description: <http://800-53.govready.com/control?id=CM-2>

Security control type: Hybrid

#### Drupal specific control support

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-03 CONFIGURATION CHANGE CONTROL

Control description: <http://800-53.govready.com/control?id=CM-3>

Security control type: Hybrid

#### CivicActions Responsibility

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.

### Part b)

#### CivicActions Responsibility

In accordance with the Configuration Management Plan, CivicActions performs security impact analysis of all planned code releases. Level of impact is assessed by CivicActions Development in collaboration with CivicActions Security 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.

### Part c)

#### CivicActions Responsibility

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.

### Part d)

#### CivicActions Responsibility

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.

### Part e)

#### CivicActions Responsibility

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.

### Part f)

#### CivicActions Responsibility

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.

### Part g)

#### CivicActions Responsibility

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-03 (2) TEST / VALIDATE / DOCUMENT CHANGES

Control description: <http://800-53.govready.com/control?id=CM-3>

Security control type: Hybrid

#### CivicActions Responsibility

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-04 SECURITY IMPACT ANALYSIS

Control description: <http://800-53.govready.com/control?id=CM-4>

Security control type: Hybrid

#### LINCS specific control or LINCS Responsibility

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

#### CivicActions Responsibility

Security impact analysis is conducted and documented within the Change Request (CR) process described in 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-05 ACCESS RESTRICTIONS FOR CHANGE

Control description: <http://800-53.govready.com/control?id=CM-5>

Security control type: Hybrid

#### CivicActions Responsibility

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 encrypted SSH session with public-key authentication, and all server access is logged.

#### Amazon Web Services (AWS) US-East/West control support

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.

## CM-05 (1) AUTOMATED ACCESS ENFORCEMENT / AUDITING

Control description: <http://800-53.govready.com/control?id=CM-5>

Security control type: Hybrid

#### Drupal specific control support

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.

All access to 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.

#### Amazon Web Services (AWS) US-East/West control support

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.

## CM-05 (5) LIMIT PRODUCTION / OPERATIONAL PRIVILEGES

Control description: <http://800-53.govready.com/control?id=CM-5>

Security control type: Hybrid

### Part a)

#### Drupal specific control support

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).

### Part b)

#### CivicActions Responsibility

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

## CM-06 CONFIGURATION SETTINGS

Control description: <http://800-53.govready.com/control?id=CM-6>

Security control type: Hybrid

#### Drupal specific control support

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.

#### Amazon Web Services (AWS) US-East/West control support

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.

### Part a)

#### LINCS specific control or LINCS Responsibility

The LINCS Technology 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. The Department 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.

### Part b)

#### LINCS specific control or LINCS Responsibility

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

#### CivicActions Responsibility

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

### Part c)

#### LINCS specific control or LINCS Responsibility

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.

### Part d)

#### CivicActions Responsibility

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-07 LEAST FUNCTIONALITY

Control description: <http://800-53.govready.com/control?id=CM-7>

Security control type: Hybrid

### Part a)

#### Amazon Web Services (AWS) US-East/West control support

Access from the internet to the application running on AWS Managed Cloud is permitted only on port 80 TCP (HTTP) and port 443 TCP (HTTPS) for Drupal, and on port 22 TCP (SSH) for the underlying web server. AWS has access to all open ports on all other computing nodes within AWS Managed Cloud to monitor internal-facing services.

### Part b)

#### LINCS specific control or LINCS Responsibility

The LINCS Technology Project maintains strict default deny policy with on 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.

#### Amazon Web Services (AWS) US-East/West control support

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

## CM-08 INFORMATION SYSTEM COMPONENT INVENTORY

Control description: <http://800-53.govready.com/control?id=CM-8>

Security control type: Hybrid

#### Drupal specific control support

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.

#### Amazon Web Services (AWS) US-East/West control support

Platform Software

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.

## CM-08 (1) UPDATES DURING INSTALLATIONS / REMOVALS

Control description: <http://800-53.govready.com/control?id=CM-8>

Security control type: Hybrid

#### CivicActions Responsibility

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.

#### Amazon Web Services (AWS) US-East/West control support

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.

## CM-09 CONFIGURATION MANAGEMENT PLAN

Control description: <http://800-53.govready.com/control?id=CM-9>

Security control type: Hybrid

#### LINCS specific control or LINCS Responsibility

The LINCS Configuration Management Plan addresses roles, responsibilities, and configuration management processes and procedures. It defines the configuration items for the information system throughout the system development life cycle and a process for managing the configuration of the configuration items.

## CM-10 SOFTWARE USAGE RESTRICTIONS

Control description: <http://800-53.govready.com/control?id=CM-10>

Security control type: Hybrid

#### Drupal specific control support

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.

#### Amazon Web Services (AWS) US-East/West control support

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.

## CM-11 USER-INSTALLED SOFTWARE

Control description: <http://800-53.govready.com/control?id=CM-11>

Security control type: Hybrid

### Part a)

#### CivicActions Responsibility

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.

#### Amazon Web Services (AWS) US-East/West control support

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.

### Part b)

#### CivicActions Responsibility

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

#### Amazon Web Services (AWS) US-East/West control support

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.

### Part c)

#### CivicActions Responsibility

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.

#### Amazon Web Services (AWS) US-East/West control support

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.