# Reusable Component Library System Security Plan

# NIST SP 800-53 Revision 4

## AC: Access Control

### AC-1: Access Control Policy And Procedures

The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and b. Reviews and updates the current: 1. Access control policy [Assignment: organization-defined frequency]; and 2. Access control 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 an access control 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 Access Control (AC) Policy. This document can be found in the CivicActions Compliance Docs GitHub repository at <https://github.com/CivicActions/compliance-docs>.

### AC-2: Account Management

The organization: a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types]; b. Assigns account managers for information system accounts; c. Establishes conditions for group and role membership; d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts; f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]; g. Monitors the use of information system accounts; h. Notifies account managers: 1. When accounts are no longer required; 2. When users are terminated or transferred; and 3. When individual information system usage or need-to-know changes; i. Authorizes access to the information system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Other attributes as required by the organization or associated missions/business functions; j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

##### 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 account management.

#### a

##### AWS

AWS Identity and Access Management (IAM) provides fine-grained access to AWS resources Operations, in collaboration with the Security Office, will set up privileged accounts accounts for the following roles: • Reporter - account that has read-only access to system reporting. • Administrator - account with full site management access.

##### Drupal

Drupal provides user accounts for individuals who participate in visiting, contributing to and administering the site with the following roles: • Anonymous user – readers of the site who either do not have an account or are not logged in. • Authenticated user – All non-anonymous users inherit the “authenticated user role.” • Administrator - This role has all permissions enabled by default.

##### SSH

Operations, in collaboration with the Security Office, will set up privileged accounts accounts for the following roles: • Developer - user level account that has access to application features and sanitized databases • System Administrator - user accounts that enjoy full system administrator (sudo) access

#### b

##### CivicActions

CivicActions’ Project Manager assigns the “admininstrator” role for the management of all accounts issued to internal admin roles supporting the information system. Account requests are initiated by the Project Manager by completing a ticket request and the CivicActions Operation Team manages the entire account creation process.

#### d

##### CivicActions

All accounts issued for application administrators and SSH are documented in CivicActions’ ticketing system. Account request tickets contain details that explain the attributes for the account including authorized users of Drupal, system infrastructure, group and role membership, and access authorizations.

##### Drupal

Drupal has a sophisticated permissions and role-based access control built in. Each role within Drupal can only access the documents and controls for which their privilege allows.

#### e

##### CivicActions

All accounts issued for the admin management of Application or SSH access must be approved by the System Owner or Project Manager who must create an account request. The CivicActions Operations Team applies appropriate account permissions and settings based on the job role and function documented within the request ticket using processes defined by the CivicActions Security Team.

#### f

##### CivicActions

CivicActions Operations is responsible for the following account management activities for both internal administrative users and customer accounts: • Establishing account justification • Activating accounts • Modifying accounts • Expiring accounts • Disabling accounts • Removing accounts

#### g

##### CivicActions

All CivicActions systems log the usage of information accounts.

##### Drupal

Drupal monitors the usage of information accounts in the watchdog.log.

#### h

##### CivicActions

In accordance with the CivicActions Access Control (AC-01) Policy when an account is no longer required, the Project Manager notifies the Operations Team to immediately disable all access. Users upon reassignment, change in roles, termination, or leaving employment are initially removed from all roles and groups, effectively denying them all access to privileged accounts.

#### i

##### CivicActions

System accounts require access authorizations prior to accounts being created. The Project Manager must initiate an access request for an account to be created. CivicActions Operations reviews the request to ensure accuracy, including intended system usage and other attributes of the user access being requested.

#### j

##### CivicActions

All privileged accounts are reviewed by CivicActions Operations every 180 days.

#### k

##### CivicActions

In accordance with standard security best practices and CivicActions policy, shared and reissued accounts for internal accounts of any kind are not created nor used for any purpose in any system.

### AC-3: Access Enforcement

The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

##### 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 account management.

##### Drupal

Access control in Drupal is enforced by authentication via unique username/password for every type of user except Anonymous user. The user’s privileges, permissions and access are provided on “least privilege” principle. The anonymous user role has the least access to the site of all roles. The website does not allow anonymous users to register an account for themselves. Drupal Administrators are the only user roles that can create new user accounts.

### AC-6: Least Privilege

The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

##### AWS

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

##### CivicActions

CivicActions performs regular audits of privileged users as part of the practice of enforcing least privilege.

##### Drupal

CivicActions implements the policy of least privilege for all logical components of Drupal by allowing only authorized access for users, which are necessary to accomplish assigned tasks in accordance with business functions and organizational need. At the application layer, Drupal is designed with a role based user access system, a least privileged approach based on assignment of privileges to roles. Drupal‘s permission systems enables control of what users can do and see on the site. CivicActions has defined a specific set of permissions for each of the user roles mentioned in control AC-5. SSH access is provided on a least privilege basis and analyzed on an ongoing basis, at least quarterly. Findings related to these audits of accounts are reported and reviewed by the CivicActions Data team and evaluated to determine roles that need to be revoked.

##### SSH

SSH access is provided on a least privilege basis and analyzed on an ongoing basis, at least quarterly. Findings related to these audits of accounts are reported and reviewed by the Security Office and evaluated to determine roles that need to be revoked.

### AC-6 (9): Auditing Use Of Privileged Functions

The information system audits the execution of privileged functions.

##### Drupal

CivicActions, at least quarterly, audits all team accounts based on the concept of least privilege. Each member of the developer team is assigned a role of which defines access needed to perform only the member’s job function. The audit of accounts is reported and reviewed by the CivicActions Operations and evaluated to determine whether roles or membership within the developer team should be changed.

### AC-7: Unsuccessful Logon Attempts

The information system: a. Enforces a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and b. Automatically [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next logon prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded.

##### AWS

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

#### a

##### Drupal

Drupal can be configured to lock an account after a specified number of invalid login attempts within specified time period.

#### b

##### Drupal

Lock down following unsuccessful attempts is configurable by Drupal administrators to conform to defined requirements. When a user exceeds the limit of invalid logon attempts, their account is automatically locked for a specfied time and requires administrator action to unlock the account before the lockout period expires.

### AC-14: Permitted Actions Without Identification Or Authentication

The organization: a. Identifies [Assignment: organization-defined user actions] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

##### Drupal

The anonymous user role has the least access to the site of all roles. The website does not allow anonymous users to register an account for themselves.

### AC-17: Remote Access

The organization: a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorizes remote access to the information system prior to allowing such connections.

##### AWS

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

##### CivicActions

The CivicActions Access Control (AC) policy defines policy for remote usage restrictions. The Project Manager or System Owner may additionally provision users according to their Access Control policies.

### AC-18: Wireless Access

The organization: a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and b. Authorizes wireless access to the information system prior to allowing such connections.

##### AWS

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

##### CivicActions

This control is not applicable. The system does not provide wireless access points.

### AC-19: Access Control For Mobile Devices

The organization: a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and b. Authorizes the connection of mobile devices to organizational information systems.

##### AWS

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

##### CivicActions

This control is not applicable. The system does not maintain a facility in which mobile device access limitations are required.

### AC-20: Use Of External Information Systems

The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: a. Access the information system from external information systems; and b. Process, store, or transmit organization-controlled information using external information systems.

##### AWS

The system inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: use of external information systems.

##### CivicActions

This control is not applicable. The system does not connect with external information systems.