# Reusable Component Library System Security Plan

# NIST SP 800-53 Revision 4

## IA: Identification and Authentication

### IA-1: Identification And Authentication Policy And Procedures

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

**Status:** Partial

**Summary:** Partially inherited from AWS (FedRAMP).

##### CivicActions

CivicActions has developed, documented and disseminated to personnel an identification and authentication 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 by the CivicActions Identification and Authentication (IA) Policy. This document can be found in the CivicActions GitHub repository at <https://github.com/CivicActions/compliance-docs>.

### IA-2: Identification And Authentication (Organizational Users)

The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

##### AWS

AWS built-in features of Identity and Access Management (IAM) provides the capability for uniquely identifying and authenticating users and processes acting on their behalf to both organizational and non-organizational users operating within the AWS account and infrastructure, providing privileges based on the credentials, group memberships, and access policies assigned to them. The customer organization, at its discretion, provides individual user accounts and privileges to both organizational non-organizational users in addition to organizational users.

### IA-2 (1): Network Access To Privileged Accounts

The information system implements multifactor authentication for network access to privileged accounts.

**Status:** Complete

##### CivicActions

CivicActions system administrators employ a personal public- key pair for basic access and must originate from a whitelisted IP address. The whitelist is maintained by an Ansible inventory file, the current complete list (includes dev sites) of users with whitelisted IPs is in artifact: None

To access root (sudo) privileges an additional password is required. The passwords are maintained in encrypted form in the Ansible inventory file. The mechanism to enable select users to use a password to obtain root access can be viewed in artifact: None

##### Drupal

Drupal administrators and other roles with unrestricted access to live content and/or user accounts are required to use two-factor authentication. See artifact None

### IA-4: Identifier Management

The organization manages information system identifiers by:  
 a. Receiving authorization from [Assignment: organization-defined personnel  
or roles] to assign an individual, group, role, or device identifier;  
 b. Selecting an identifier that identifies an individual, group, role, or device;  
 c. Assigning the identifier to the intended individual, group, role, or device;  
 d. Preventing reuse of identifiers for [Assignment: organization-defined time  
period]; and  
 e. Disabling the identifier after [Assignment: organization-defined time period  
of inactivity].

**Status:** Partial

**Summary:** Partially inherited from AWS (FedRAMP).

#### a

##### CivicActions

Access to the system is authorized by the System Owner or Project Manager for each role as described in AC-2.

##### Drupal

Upon account creation, the Drupal software assigns each user account a unique numerical user ID (UID). This UID is used internally by the system to track user actions such as content creation or editing. The numerical user IDs are never reused even if their user accounts are subsequently blocked or deleted.

#### b

##### CivicActions

User accounts are assigned a unique identifier in the form of a unique username, password and email address based on the system for allocating user accounts described in AC-2.

In accordance with CivicActions Identification and Authentication (IA) Policy outlined at <https://github.com/CivicActions/compliance-docs>, CivicActions internal users are uniquely identified by the creation of an organizational account with a username based on each user’s first and last names.

##### Drupal

When Drupal user accounts are created, users’ email addresses are verified by sending a single-use activation link to the user’s mailbox. The email recipient then uses the activation link to log in to the website and supply a password which must meet the system’s password complexity requirements.

#### c

##### CivicActions

User accounts are assigned a unique identifier in the form of a unique username, password and email address based on the system for allocating user accounts described in AC-2.

##### Drupal

Identifiers for CivicActions internal personnel include a username based on the individual’s full first and last name and are reviewed for uniqueness by the admin group when it approves the creation of the user account.

#### d

##### CivicActions

Account usernames may not be re-used for at least two years.

##### Drupal

Drupal user’s unique identifier (the numeric user ID, or UID) is never reused.

#### e

##### CivicActions

All user accounts are required to change their passwords every 90 days. The website will automatically block the accounts of users who fail to change their password within that time period, after which the account may only be unblocked by a website Administrator or CivicActions Operations staff.

### IA-5: Authenticator Management

The organization manages information system authenticators by:  
 a. Verifying, as part of the initial authenticator distribution, the identity  
of the individual, group, role, or device receiving the authenticator;  
 b. Establishing initial authenticator content for authenticators defined by  
the organization;  
 c. Ensuring that authenticators have sufficient strength of mechanism for their  
intended use;  
 d. Establishing and implementing administrative procedures for initial authenticator  
distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;  
 e. Changing default content of authenticators prior to information system installation;  
 f. Establishing minimum and maximum lifetime restrictions and reuse conditions  
for authenticators;  
 g. Changing/refreshing authenticators [Assignment: organization-defined time  
period by authenticator type];  
 h. Protecting authenticator content from unauthorized disclosure and modification;  
 i. Requiring individuals to take, and having devices implement, specific security  
safeguards to protect authenticators; and  
 j. Changing authenticators for group/role accounts when membership to those  
accounts changes.

**Status:** Partial

**Summary:** Partially inherited from AWS (FedRAMP).

#### a

##### Drupal

Refer to control AC-2 in this SSP for further details on account provisioning. CivicActions will create and maintain an initial Drupal Administrator (highest level of Drupal Account). New Administrators are able to provide additional Administrator access at their own discretion and are ultimately responsible for managing their own Administrator and other user accounts that they create.

#### b

##### Drupal

Initial authenticator content (a unique email address – not previously used in any other account) is provided by the user. Internal initial password requirements set by CivicActions Operations and ongoing password refreshes by internal users follow the requirements set in the Identification and Authentication Policy.

#### c

##### Drupal

The system partially inherits this control from Drupal standard password strength mechanisms.

#### d

##### Drupal

The system partially inherits this control from Drupal standard password management. All password creation/change/reset operations are recorded in the website’s “Drupal Watchdog” logs.

#### e

##### Drupal

Drupal requires users to change their password upon initial login, and the application website enforces this. Each user account is assigned a default password that is randomly generated, not possible to guess, and not shared with anyone, including site administrators. When the user logs in and creates a new password, the default password is erased from the website database.

#### h

##### Drupal

For all Drupal users, passwords are protected by the website’s software, which only stores an encrypted string based on the password. This means that even if the website’s database should be compromised, an attacker would still be unable to know users’ actual passwords. Internal users receive training in security awareness and acceptable use and are instructed never to reveal their passwords to anyone.

#### i

##### CivicActions

CivicActions users are required to take appropriate measures in the handling of passwords including:

* Not transmitting user names and passwords together in an unencrypted format
* Not permitting the sending of passwords in an unencrypted format via email
* Not listing passwords in tickets
* Not writing down or storing passwords in a readable form in any physical or logical location where they may be discoverable by unauthorized persons.

##### Drupal

Drupal users are required to take appropriate measures in the handling of passwords including:

* Not transmitting user names and passwords together in an unencrypted format
* Not permitting the sending of passwords in an unencrypted format via email
* Not listing passwords in tickets
* Not writing down or storing passwords in a readable form in any physical or logical location where they may be discoverable by unauthorized persons.

#### j

##### Drupal

This control is not applicable due to the fact that group accounts are not created within the Drupal application per IA Policy.

### IA-5 (1): Password-Based Authentication

The information system, for password-based authentication:  
 (1)(a). Enforces minimum password complexity of [Assignment: organization-defined  
requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type];  
 (1)(b). Enforces at least the following number of changed characters when  
new passwords are created: [Assignment: organization-defined number];  
 (1)(c). Stores and transmits only cryptographically-protected passwords;  
 (1)(d). Enforces password minimum and maximum lifetime restrictions of [Assignment:  
organization-defined numbers for lifetime minimum, lifetime maximum];  
 (1)(e). Prohibits password reuse for [Assignment: organization-defined number]  
generations; and  
 (1)(f). Allows the use of a temporary password for system logons with an immediate  
change to a permanent password.

**Status:** Partial

**Summary:** Partially inherited from AWS (FedRAMP).

#### a

##### AWS

AWS built-in features of Identity and Access Management (IAM) provides minimum password complexity enforcement, but the characteristics to enforce must be manually configured by the customer. Refer to http://docs.aws.amazon.com/IAM/latest/UserGuide/id\_credentials\_passwords\_account-policy.html

##### Drupal

Drupal supports the requirement for password-based authentication complexity. New users of Drupal are required to specify their password authentication as soon as they log in to the website for the first. The website requires all submitted passwords to comply with validation rules, as described above in IA-5(c). Changing password lifetime, length, reuse or strength requirements requires a code setting change that therefore needs to be planned and approved by CivicActions Change Control Board before being implemented.

#### b

##### Drupal

When required to change passwords, Drupal users are required to change their authenticator password by changing at least one character. Enforcement of this control is implemented through the website’s software configuration.

#### c

##### AWS

AWS built-in features of AWS Identity and Access Management (IAM) and the AWS Console store passwords on AWS systems in a cryptographically-protected format and only support TLS connectivity to the console web site to protect passwords in transit via encryption.

##### Drupal

All Drupal passwords are encrypted in storage, using the SHA-512 hashing algorithm with a salt. The hash function is performed repeatedly to further obfuscate the password via key stretching. In transmission, passwords are encrypted using SSL via HTTPS.

#### d

##### Drupal

The website requires all submitted passwords to comply with lifetime rules, as described above in IA-5(g).

#### e

##### Drupal

Password reuse is limited through software configuration.

#### f

##### AWS

AWS built-in features of AWS Identity and Access Management (IAM) provides the capability to require new password to be entered upon login. The customer organization, at its discretion, configures IAM to enforce that requirement.

##### Drupal

When website users request a password reset, the website sends a temporary login link to the email address associated with their user account. After a user logs in via the temporary login link, the website requires the user to enter a new password before proceeding further.

### IA-5 (11): Hardware Token-Based Authentication

The information system, for hardware token-based authentication, employs mechanisms that satisfy [Assignment: organization-defined token quality requirements].

**Status:** Complete

##### AWS

AWS built-in features of AWS Identity and Access Management (IAM) provides the capability for Hardware MFA using Gemalto SafeNet IDProve 100 and 700 OTP Tokens which are compliant to OATH open standard (time based - 6 digits) Expected battery life is 3-5 years or approximately 15,000 - 20,000 clicks. These products are handheld devices that provide strong authentication by generating a unique password that is valid for only one attempt and for 30 seconds.

It is the customer organization’s responsibility to implement Hardware MFA. Refer to http://aws.amazon.com/iam/details/mfa/ and http://docs.aws.amazon.com/IAM/latest/UserGuide/id\_credentials\_mfa.html

### IA-6: Authenticator Feedback

The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

**Status:** Complete

##### AWS

In this architecture, All EC2 instances (bastion host, web/proxy servers, application servers) employ SSH for interactive login, and when a key passphrase is prompted for, the SSH prompting mechanism obscures the feedback by default.

AWS built-in features obscure keystroke feedback for password input during AWS console login with AWS Identity and Access Management (IAM) user credentials, and when the CloudFormation console prompts for an initial database password during Quick Start template deployment.

##### Drupal

Feedback of authentication information is obscured during the authentication process into the Drupal application by displaying “dots” in the place of a password, as is standard for web-based applications. In transmission, passwords are encrypted using SSL via HTTPS.

### IA-7: Cryptographic Module Authentication

The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

**Status:** Complete

##### AWS

AWS built-in features of AWS Identity and Access Management (IAM) authentication employs cryptographic modules that meet requirements as specified and assessed in the AWS FedRAMP authorization package.

##### Drupal

All Drupal passwords are encrypted in storage, using the SHA-512 hashing algorithm with a salt. SHA-512 is an approved security function under FIPS PUB 140-2. The hash function is performed repeatedly to further obfuscate the password via key stretching. In transmission, passwords are encrypted using SSL via HTTPS.

#### j

##### CivicActions

CivicActions systems employ authentication methods consistent with NIST FIPS 140-2 requirements. General public access to system web pages does not require cryptographic authentication. Privileged users accessing systems use the public-key cryptographic functionality of Secure Shell (SSH) to encrypt the exchange of information (including the password) between the remote user and the server. Where Transport Layer Security (TLS, aka SSL) is used, cryptographic modules will be configured in accordance with FIPS 140-2.

### IA-8: Identification And Authentication (Non-Organizational Users)

The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

##### AWS

AWS built-in features of AWS Identity and Access Management (IAM) provide the capability for uniquely identifying and authenticating users and processes acting on their behalf to both organizational and non-organizational users, providing privileges based on the credentials, group memberships, and access policies assigned to them.

The customer organization at its discretion provides user accounts and privileges to both organizational non-organizational users in addition to organizational users.