# Reusable Component Library System Security Plan

# NIST SP 800-53 Revision 4

## PS: Personnel Security

### PS-1: Personnel Security Policy And Procedures

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

##### AWS

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

##### CivicActions

CivicActions has developed, documented and disseminated to personnel a personnel security 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 CivicActions Personnel Security (PS) Policy document that can be found in the CivicActions Github repository at <https://github.com/CivicActions/compliance-docs>.

### PS-2: Position Risk Designation

The organization: a. Assigns a risk designation to all organizational positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and updates position risk designations [Assignment: organization-defined frequency].

#### a

##### CivicActions

Risk designations are assigned to all CivicActions positions. The CivicActions Director of Human Resources works in coordination with the CivicActions ISSO and the Chief Operating Officer to assign risk designations.

#### b

##### CivicActions

The CivicActions Director of Human Resources works in coordination with the CivicActions ISSO and the Chief Operating Officer to establish screening criteria for all CivicActions positions.

#### c

##### CivicActions

At least every three (3) years, the CivicActions Director of Human Resources reviews and revises position risk designations. If the Director of Human Resources determines that significant changes must be made to the position risk descriptions the Director of Human Resources works in coordination with the CivicActions ISSO and the Chief Operating Officer to implement changes as required.

### PS-3: Personnel Screening

The organization: a. Screens individuals prior to authorizing access to the information system; and b. Rescreens individuals according to [Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening].

#### a

##### CivicActions

Prospective CivicActions employees undergo background checks commensurate with the individual’s job duties, the classification of the information they will access, and the risks associated with the role. At the discretion of the Chief Operating Officer these checks may also be conducted on contractors and / or third party users in cases where they will have access to application data that is not meant to be consumed by the public. In these instances, the Chief Operating Officer will instruct the Director of Human Resources to conduct a background check before granting access to the information system.

#### b

##### CivicActions

Rescreening is conducted as required by the individual’s job duties, the classification of the information they will access, and the risks associated with the role. A basic background check is performed for all CivicActions employees.

### PS-4: Personnel Termination

The organization, upon termination of individual employment: a. Disables information system access within [Assignment: organization-defined time period]; b. Terminates/revokes any authenticators/credentials associated with the individual; c. Conducts exit interviews that include a discussion of [Assignment: organization-defined information security topics]; d. Retrieves all security-related organizational information system-related property; e. Retains access to organizational information and information systems formerly controlled by terminated individual; and f. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].

#### a

##### CivicActions

Information system access is terminated immediately upon the voluntary or involuntary departure of an employee. In the case of involuntary departure, in addition to immediate termination of system access, at no point is a departing employee allowed access to any part of the CivicActions infrastructure. In the case of voluntary departure, employees are permitted access to the information system for the duration of their off boarding period. The departing employee’s manager is responsible for informing the Information Technology department when the employee off boarding period concludes. At this time system and facility access is terminated.

#### b

##### CivicActions

The terminated user’s accounts are disabled and all access associated with the individual is revoked.

#### c

##### CivicActions

The employee’s manager or the Director of Human Resources conducts exit interviews with all employees who leave CivicActions voluntarily. There is a general discussion about the process of turning in any/all company issued devices, laptops, etc.

#### d

##### CivicActions

CivicActions employees provide their own equipment that must be hardened to security reqirements depending upon their role and duties. CivicActions supplies two factor authentication tokens that become the property of the employee. Some employees may receive company-issued hardware for working on particular projects. These items are collected before the employee exits CivicActions. In the case of an involuntary termination, the Director of Human Resources works to collect company issued devices and provides paperwork highlighting confidential protections for customers.

#### e

##### CivicActions

Access to CivicActions information and information systems is always shared, so that the termination of an individual will not prevent CivicActions from having access to needed resources.

#### f

##### CivicActions

When a person is terminated, a standard off-boarding process is used to notify management and IT and to track the process of disabling access to the information system/information system components. CivicActions IT Operations and Security is given at least a four hour notice to schedule the deactivation of access upon termination. Deactivation is a manual process that is tracked via a Trello card in order to meet the four hour turnaround time before termination.

### PS-5: Personnel Transfer

The organization: a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization; b. Initiates [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action]; c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and d. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].

#### a

##### CivicActions

When an employee, third party personnel and / or contractor is transferred to a new project or position within CivicActions, they may maintain access to the previous system they were working on in order to facilitate the process of maintenance and knowledge transfer. However, as part of the practices of account management (AC-2) and least privilege (AC-6), regular audits of privileged users are conducted and access privileges may be removed when no longer needed. Additionally, adherence to specific client SLAs may enhance the frequency of such audits or the timeliness of privilege removal during personnel transfer.

#### b

##### CivicActions

When an employee, third party personnel and / or contractor is transferred to a new position within CivicActions and there is a requirement for access change, such access changes are normally completed within five business days.

#### c

##### CivicActions

Access authorizations are modified as needed to coincide with changes in duties or operational need upon personnel transfer or reassignment.

#### d

##### CivicActions

CivicActions Operations is informed of transfers that require access authorization modifications within five business days by the Project Manager, System Owner or Director of Human Resources.

### PS-8: Personnel Sanctions

The organization: a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and b. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

#### a

##### CivicActions

CivicActions Security and/or the Director of Human Resources is responsible for determining and enforcing sanctions for failing to comply with established information security policies and procedures. Coaching may be considered prior to sanctions. Sanctions may include but are not limited to written warnings, reduction in system access, demotion, or termination.

#### b

##### CivicActions

When employee sanctions processes are initiated, the Director of Human Resources notifies the respective Project Manager(s) and CivicActions Security within five business days.