# 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>.

##### Project

The Project documents the security policy and procedures in addressing position categorization, personnel screening, personnel termination, personnel transfer, and access agreements within the Project SSP. Project adopts the Client personnel security standards and determines position risks levels based on public trust responsibilities.

This is Agency common control. More data about implementation can be obtained from the Agency common control catalog.

### 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].

##### Project

Project position sensitivity levels are assigned by the Client Full Name. Each position designation is documented on the Standard Position Description (SPD) and assigned a risk level (or sensitivity level) commensurate with the sensitivity of the information, the risk to that information and the system maintaining that information. The levels of risk still need to be designated by Client for employee and contractor positions but since Project system does not have any sensitive data, a low risk scenario can be assumed.

* Employee risk levels and background investigations are: Low Risk= NACI, Moderate Risk= LBI, High Risk= BI.
* Contractor risk levels and background investigations are: Low Risk= NACI, Moderate Risk= NACC, High Risk= BI.

In order to ensure every employee is assigned to a position, which has been reviewed for sensitivity by the NCC, the SPD is a required data attribute of an employee’s HR record. Position risks designations are reviewed and revised when NCC or OPM publish changes to sensitivity levels.

This is Agency common control. More data about implementation can be obtained from the Agency common control catalog

#### a

##### CivicActions

Risk designations are assigned to all CivicActions positions. The CivicActions Office of Human Resources works in coordination with the CivicActions Security Office to assign risk designations.

#### b

##### CivicActions

The CivicActions Office of Human Resources works in coordination with the CivicActions Security Office to establish screening criteria for all CivicActions positions.

#### c

##### CivicActions

At least every three (3) years, the CivicActions Office of Human Resources reviews and revises position risk designations. If the Office of Human Resources determines that significant changes must be made to the position risk descriptions the Office of Human Resources works in coordination with the CivicActions Security Office 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].

##### Project

Minimum background investigations are conducted, since all data is non-sensitive, for individuals requiring access to Project information and information systems. The type of background investigation conducted for an individual is determined by the individual’s position risk categorization noted in control PS-2. Client conducts periodic reinvestigations in accordance with OPM and NIST guidelines.

This is Agency common control. More data about implementation can be obtained from the Agency common control catalog.

#### 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 CivicActions Security Office, 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 Security Office will instruct the Office 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].

##### Project

Client Full Name HR policy states that managers or designated officials are responsible for recovering and properly securing employee badges and returning it to the local physical security office. The Client executes termination procedures that remove personnel access privileges, computer accounts. When an employee is terminated, the employee’s manager or designated official completes a form requesting termination of access for the user. Local management and the security manager coordinate disabling or removing Project privileged access with the system administrator. The employee’s manager or designated official is responsible for recovering and properly securing his/her ID badge and returning it to the local physical security office. The employee’s manager or designated official ensures that any information on the system that the employee was responsible for will be available to the appropriate personnel.

This is Agency common control. More data about implementation can be obtained from the Agency common control catalog.

#### 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 offboarding period. The departing employee’s manager is responsible for informing the Information Technology department when the employee offboarding 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 Office 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 requirements depending upon their roles 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 Office 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 CivicActions’ Operations staff, and to track the process of disabling access to the information system/information system components. The CivicActions Operations staff and Security Office are given at least four hours 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].

##### Project

When an employee is reassigned or transferred, the employee’s manager or designated official is required to request transfer of access (as appropriate) for the user.

In accordance with the Client Full Name HR policy, the employee’s manager or designated official is responsible for recovering and properly securing his/her ID badge and returning it to the local physical security office. The manager provides prompt notification to the Project system/security administrator when an employee changes assignments and/or location. This includes taking prompt and appropriate action to change employee access profile and/or remove employee from the system; and ensure that users’ system access is cancelled when the need no longer exists.

This is Agency common control. More data about implementation can be obtained from the Agency common control catalog.

#### 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 needs upon personnel transfer or reassignment.

#### d

##### CivicActions

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

### PS-6: Access Agreements

The organization:  
 a. Develops and documents access agreements for organizational information  
systems;  
 b. Reviews and updates the access agreements [Assignment: organization-defined  
frequency]; and  
 c. Ensures that individuals requiring access to organizational information  
and information systems:  
 1. Sign appropriate access agreements prior to being granted access; and  
 2. Re-sign access agreements to maintain access to organizational information  
systems when access agreements have been updated or [Assignment: organization-defined frequency].

#### a

##### Project

All users of the Project system must read and accept access agreements upon every login.

#### b

##### Project

The Access Agreements are reviewed at least annually or when a significant change occurs.

#### c

##### Project

All individuals requiring access to the Project system are required to sign the Access Agreements before login is granted. When the Access Agreements are updated, the individual will be required to sign the new copy before regaining access.

### PS-7: Third-Party Personnel Security

The organization:  
 a. Establishes personnel security requirements including security roles and  
responsibilities for third-party providers;  
 b. Requires third-party providers to comply with personnel security policies  
and procedures established by the organization;  
 c. Documents personnel security requirements;  
 d. Requires third-party providers to notify [Assignment: organization-defined  
personnel or roles] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [Assignment: organization-defined time period]; and  
 e. Monitors provider compliance.

#### a

##### Project

Personnel security requirements including security roles and responsibilities that apply to primary contracting organizations flow down to their subcontractors.

#### b

##### Project

Personnel security policies and procedures that apply to primary contracting organizations flow down to their subcontractors.

#### c

##### Project

All personnel security requirements are documented in PS-1 and other related Personnel Security controls.

#### d

##### Project

For personnel transfers and terminations of third-party personnel, the procedures defined in employee termination (PS-4) and employee transfer (PS-5) flow down to subcontractors.

#### e

##### Project

Compliance measures for assessing third-party personnel and/or contractors are determined on a case-by-case basis. Third-party personnel are monitored to ensure compliance with personnel security requirements.

### 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.

##### Project

The disciplinary sanctions for personnel failing to comply with establish IT security policies and procedures are included in Client Full Name HR policy. If an employee violates the Client information security policies and procedures, the employee may be subject to disciplinary action at the discretion of management. Actions may range from verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or termination, depending on the severity of the violation. Disciplinary sanctions are reported to the OCIO.

#### a

##### CivicActions

The CivicActions Security Office and/or the Office 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 Office of Human Resources notifies the respective Project Manager(s) and CivicActions’ Security Office within five business days.