# PERSONNEL SECURITY

## PS-01 PERSONNEL SECURITY POLICY AND PROCEDURES

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

Security control type: Hybrid

#### LINCS specific control or LINCS Responsibility

The LINCS Technology Project documents the security policy and procedures in addressing position categorization, personnel screening, personnel termination, personnel transfer, and access agreements within the LINCS SSP. The LINCS Technology Project adopts the Department of Education 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.

#### CivicActions Responsibility

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>.

#### 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 Provider dated 1 May 2013.

## PS-02 POSITION RISK DESIGNATION

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

Security control type: Hybrid

#### LINCS specific control or LINCS Responsibility

The LINCS Technology Project’s position sensitivity levels are assigned by the Department of Education and National Classification Center (NCC) as part of the position designation required by OPM under 5 CFR 731.106. Each Department 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 the Department for employee and contractor positions but since the LINCS Technology 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

### Part a)

#### CivicActions Responsibility

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.

### Part b)

#### CivicActions Responsibility

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.

### Part c)

#### CivicActions Responsibility

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-03 PERSONNEL SCREENING

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

Security control type: Hybrid

#### LINCS specific control or LINCS Responsibility

Minimum background investigations are conducted, since all data is non-sensitive, for individuals requiring access to LINCS Technology 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. The Department 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.

### Part a)

#### CivicActions Responsibility

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.

### Part b)

#### CivicActions Responsibility

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-04 PERSONNEL TERMINATION

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

Security control type: Hybrid

#### LINCS specific control or LINCS Responsibility

The Department’s 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 Department 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 LINCS Technology 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.

### Part a)

#### CivicActions Responsibility

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.

### Part b)

#### CivicActions Responsibility

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

### Part c)

#### CivicActions Responsibility

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.

### Part d)

#### CivicActions Responsibility

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 poarticular 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.

### Part e)

#### CivicActions Responsibility

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.

### Part f)

#### CivicActions Responsibility

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-05 PERSONNEL TRANSFER

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

Security control type: Hybrid

#### LINCS specific control or LINCS Responsibility

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 Department’s 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 LINCS Technology 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.

### Part a)

#### CivicActions Responsibility

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-02) and least privilege (AC-06), 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.

### Part b)

#### CivicActions Responsibility

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.

### Part c)

#### CivicActions Responsibility

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

### Part d)

#### CivicActions Responsibility

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-06 ACCESS AGREEMENTS

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

Security control type: Hybrid

#### LINCS specific control or LINCS Responsibility

The Department has implemented a formalized process for user account administration using the approved and signed Rules of Behavior and User Acknowledgement forms. All new users requesting access to the LINCS Technology Project system must complete these forms and the security manager will keep them on file and reviewed bi-annually.

### Part a)

#### CivicActions Responsibility

CivicActions has developed and documented an Acceptable Use Policy that covers access and use of all CivicActiuons systems.

### Part b)

#### CivicActions Responsibility

The Acceptable Use Policy is reviewed at least annually or when a significant change occurs. In the event that a major update is made to the Acceptable Use Policy, employees are required to read and sign the updated policy document and Human Resources stores the information.

### Part c)

#### CivicActions Responsibility

All CivicActions team members are required to read and sign the Acceptable Use Policy (AUP) provided in the Security Policy document prior to gaining access to the any CivicActions system. The acknowledgment signature page is a separate document collected and recorded by the Director of Human Resources.

## PS-07 THIRD-PARTY PERSONNEL SECURITY

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

Security control type: Hybrid

#### LINCS specific control or LINCS Responsibility

All contractor support personnel are required to meet the same personnel security policy requirements as Department personnel who have privileged access to the LINCS Technology Project system. Third party providers are required to review and sign the Rules of Behavior prior to being granted access to the system.

### Part a)

#### CivicActions Responsibility

Third party personnel are required to following the same process and requirements as CivicActions employees.

### Part b)

#### CivicActions Responsibility

Third party personnel are required to following the same process and requirements as CivicActions employees. CivicActions Operations or Security may require that a background check 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.

### Part c)

#### CivicActions Responsibility

All personnel security requirements are documented and include things such as signing the Acceptable Use Policy (AUP) and taking security awareness training.

### Part d)

#### CivicActions Responsibility

For personnel transfers and terminations of third-party personnel with access to the CivicActions systems, third parties must notify the CivicActions Operations an/or Director of Human Resources the same day. The same employee transfer and/or termination procedure(s) are folloed as if the third party personnel were CivicActions employees.

### Part e)

#### CivicActions Responsibility

Compliance measures for assessing third-party personnel and/or contractors are determined on a case-by-case basis. CivicActions Security is responsible for coordinating with the managers of external systems to include appropriate and tailored compliance verification language in contracts as required. Third-party personnel are continuously monitored to ensure compliance with personnel security requirements.

## PS-08 PERSONNEL SANCTIONS

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

Security control type: Hybrid

#### LINCS specific control or LINCS Responsibility

The disciplinary sanctions for personnel failing to comply with establish IT security policies and procedures are included in the Department’s HR policy. If an employee violates the Department’s 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.

### Part a)

#### CivicActions Responsibility

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.

### Part b)

#### CivicActions Responsibility

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