# LINCS System Security Plan

# NIST SP 800-53 Revision 4

## AT: Awareness and Training

### AT-1: Security Awareness And Training Policy And Procedures

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

##### LINCS

Security awareness and training policy and procedures are formally documented in Department of Education, Office of the Chief Information Officer, Handbook for Information Assurance Security Policy, Information Assurance Program (Handbook OCIO-01), which provides the roles and responsibilities as it pertains to security awareness and training. The Department will ensure all users, including managers and senior executives, are exposed to basic information system security awareness materials before authorizing access to the system and at least annually thereafter. The Department documents and monitors all individual information system security training activities including basic security awareness training. The Department reviews and updates the policy as necessary.

### AT-2: Security Awareness Training

The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors): a. As part of initial training for new users; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter.

##### AWS

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

##### LINCS

The Department personnel and contractor employees involved with the management, operation, programming, maintenance, or use of LINCS Technology Project system receive training in acceptable computer security practices prior to system access. All Department employees and contractors are required to complete annual IT security awareness training. This security awareness training covers issues and policies associated with information security, including end user security roles and responsibilities and rules of behavior. Some topics addressed in the training are: \* Password protection \* System rules of behavior \* Protection of hardware, software, and data \* Proper handling of copyrighted materials \* Reporting of security breaches and violations \* Proper procedures for software installation, uploading, and use on workstations. The security and awareness training is consistent with Department of Education IT Security Training Program Plan and the guidance in NIST Special Publication 800-50.

#### a

##### CivicActions

Both regular and ad hoc training to all CivicActions personnel, including those who support the system infrastructure and applications, is provided. All employees and contractors must complete Security Awareness trainings upon being hired and at least annually thereafter. CivicActions Operations will not create accounts for individuals until they have successfully completed the trainings. Additional training will be provided as required by system changes. Training takes the following forms: Annual Knowledge Survey (i.e., Security Awareness Training): All employees are required to review trainings covering Security Awareness. After the training, a survey-style security awareness test is taken by employees. All CivicActions personnel are required to complete and pass the survey, and new employees are required to pass before being granted access to the Information System. In order to successfully pass the test, a score of 80% is required. This survey tests CivicActions personnel’s knowledge of critical security subjects, policies and procedures. Results from this survey are compiled by the Director of Human Resources and used to refine future training efforts. Ad Hoc Security Awareness: The CivicActions ISSO oversees the approximately bi-monthly distribution of security awareness tips and articles to the all CivicActions employees. This can include general tips as well as articles tailored to the specific requirements of CivicActions users.

#### b

##### CivicActions

In the event of a major system change, the Project Manager is responsible for delivering additional training to impacted personnel. Specific training type, medium and delivery method is dependent upon the nature of the system change.

#### c

##### CivicActions

CivicActions provides annual security awareness training to its personnel.

### AT-3: Role-Based Security Training

The organization provides role-based security training to personnel with assigned security roles and responsibilities: a. Before authorizing access to the information system or performing assigned duties; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter.

##### AWS

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

##### LINCS

Completion of role-based training is an annual requirement for personnel in roles with significant information security responsibilities that require specialized role-based training. Role-based cybersecurity training is developed and implemented to meet identified training needs and competencies associated with the various target audiences/functional roles (federal and contractor employees) that comprise the Department workforce, as is identified in and required by the FISMA and OMB A-130, Appendix III. The appropriate content of security training is determined based on the assigned roles and responsibilities of individuals and the specific security requirements of the Department, PO and the information systems to which personnel have authorized access. Annual training requirements may be met by completing one or more course(s) within the Department’s learning management systems, participating in instructor-led training provided by the OCIO, or completing an external role-based course or courses offered within their specific functional area of expertise.

#### a

##### CivicActions

CivicActions personnel with security responsibilities are required to complete role-based security training before being provided with access to the information system. The CivicActions ISSO is responsible for creating the content of the training. The role-based training is provided and tracked by the CivicActions Information Security Office.

#### b

##### CivicActions

The Project manager in collaboration with CivicActions Security determines whether a change to the information system requires any modifications and updates to the security awareness training program and if so, works with the CivicActions Security to implement the change.

#### c

##### CivicActions

CivicActions’ Security provides users with security responsibilities role-based security training on an annual basis. The training is provided and tracked by the CivicActions Information Security Office.

### AT-4: Security Training Records

The organization: a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and b. Retains individual training records for [Assignment: organization-defined time period].

#### a

##### CivicActions

The CivicActions Information Security Office tracks all security awareness training within the organization and ensures that all employees have successfully completed training when required. The training records are stored and tracked in a spreadsheet maintained by the CivicActions Information Security Office.

##### LINCS

The Department documents and monitors all individual information system security training activities including basic security awareness training. New users are required to take security training within 30 days of hire. This information is kept in the appropriate personnel files to verify users have met the training requirements. Training requirement notifications are sent to individuals as deadline for re-training approaches.

#### b

##### AWS

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

##### CivicActions

Training records are tracked and maintained by the CivicActions Information Security Office. Records are maintained permanently.

##### LINCS

The Office of Information Secuity maintains training certifications for the specified period.