# LINCS System Security Plan

# NIST SP 800-53 Revision 4

## PL: Planning

### PL-1: Security Planning Policy And Procedures

The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A security planning 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 planning policy and associated security planning controls; and b. Reviews and updates the current: 1. Security planning policy [Assignment: organization-defined frequency]; and 2. Security planning 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 system planning 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 Planning (PL) Policy and Procedure document that can be found in the CivicActions Github repository at <https://github.com/CivicActions/compliance-docs/>.

##### LINCS

This is Agency common control. More data about implementation can be obtained from the Agency common control catalog. The LINCS Technology Project developed its security policy planning and procedures based on the Department of Education, Office of the Chief Information Officer, Handbook for Information Assurance Security Policy, Information Assurance Program (Handbook OCIO-01), guidance from NIST, the Office of Management and Budget and industry best practices. Security policies and procedures are formally documented within the LINCS SSP, which provides the roles and responsibilities as it pertains to security planning. It provides guidance on all aspects of security for the protection of LINCS information technology resources. It defines responsibilities for the implementation and oversight of the guidance contained herein. The plan was last updated in December, 2015.

### PL-2: System Security Plan

The organization: a. Develops a security plan for the information system that: 1. Is consistent with the organization�s enterprise architecture; 2. Explicitly defines the authorization boundary for the system; 3. Describes the operational context of the information system in terms of missions and business processes; 4. Provides the security categorization of the information system including supporting rationale; 5. Describes the operational environment for the information system and relationships with or connections to other information systems; 6. Provides an overview of the security requirements for the system; 7. Identifies any relevant overlays, if applicable; 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and 9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Distributes copies of the security plan and communicates subsequent changes to the plan to [Assignment: organization-defined personnel or roles]; c. Reviews the security plan for the information system [Assignment: organization-defined frequency]; d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and e. Protects the security plan from unauthorized disclosure and modification.

##### AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: AWS system security plan.

##### LINCS

The System Security Plan (SSP) was developed and implemented for LINCS Technology Project system in accordance with the Department of Education, Office of the Chief Information Officer, Handbook for Information Assurance Security Policy, Information Assurance Program (Handbook OCIO-01), Department of Education Information Technology Security, Handbook for Information Technology Security, Certification and Accreditation Procedures (Handbook OCIO-05), NIST SP 800-18 and NIST SP 800-37. The SSP includes a description of the management, operational, and technical controls in place or planned for the application. The SSP is included as a key document in an application’s C&A package and is reviewed and approved by designated officials. The SSP identifies the system owner and responsible parties for managing system access and the overall security of the system. The Chief Information Security Officer reviews and approves the SSP. The SSP will be reviewed at least annually and updated to account for any changes to the LINCS system and to address any changes in security controls.

#### a

##### CivicActions

CivicActions has developed this system security plan (SSP) for the information system as part of compliance with NIST 800-53 and FIPS 199. The SSP defines the security categorization, system boundary, and security requirements and controls meeting the requirements of the NIST Risk Management Framework (RMF). Specifically the SSP: 1. Is consistent with the organization’s enterprise architecture 2. Explicitly defines the authorization boundary for the system 3. Describes the operational context of the information system in terms of missions and business processes 4. Provides the security categorization of the information system including supporting rationale 5. Describes the operational environment for the information system and relationships with or connections to other information systems 6. Provides an overview of the security requirements for the system 7. Identifies any relevant overlays, if applicable 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions 9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation

#### b

##### CivicActions

The SSP is reviewed and approved by the authorizing official prior to plan implementation. A copy of the SSP is provided to authorized CivicActions and assessing personnel including the System Owner, Authorizing Official, Information System Security Officer, System/Network Administrator and CivicActions Operations. The SSP is maintained by CivicActions Security.

#### c

##### CivicActions

The SSP is reviewed at least annually by the System Owner and CivicActions Operations in collaboration with CivicActions Security.

#### d

##### CivicActions

CivicActions Operations in collaboration with CivicActions Security updates the system description and control descriptions within the SSP as needed to verify the SSP is an accurate description of the system.

#### e

##### CivicActions

The SSP is currently available to authorized users on GitLab. Per the Acceptable Use Policy, all entities granted access to CivicActions information assets are required to complete a non-disclosure agreement (NDA) to uphold information confidentiality. GitLab provides the configuration management capabilities for the SSP to be protected from unauthorized disclosure and modification.

### PL-4: Rules Of Behavior

The organization: a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; b. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system; c. Reviews and updates the rules of behavior [Assignment: organization-defined frequency]; and d. Requires individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.

##### LINCS

All users (privileged and program account users) requesting access to the LINCS Technology Project system are required to read the LINCS’ Rules of Behaviors, complete an account request form and sign both documents. Appendix B includes the Rules of Behavior, describing the user’s responsibilities and expected behavior when using the application and also includes the User Acknowledgement form. Account management procedures are described in detail in the SSP.

#### a

##### CivicActions

CivicActions maintains an Acceptable Use Policy that all CivicActions personnel are required to abide by when working with CivicActions operated systems. This information is available in the CivicActions Handbook under Security Policy here: <https://civicactions-handbook.readthedocs.io/en/latest/03-policies/security/#acceptable-use-policy>.

#### b

##### CivicActions

All CivicActions employees are required to read and sign the Security Policy <https://civicactions-handbook.readthedocs.io/en/latest/03-policies/security/> which includes the Acceptable Use Policy, prior to being authorized access to CivicActions operated systems. This is part of the onboarding Security Training process: <https://civicactions-handbook.readthedocs.io/en/latest/01-welcome-to-civicactions/training/security-training/> If CivicActions staff fail to comply with CivicActions security awareness and training requirements, their access to CivicActions information systems may be terminated.

#### c

##### CivicActions

The CivicActions Acceptable Use Policy/Rules of Behavior are reviewed by CivicActions Security and Operations at least annually and is updated at least every three years.

#### d

##### CivicActions

CivicActions employees re-sign the revised/updated Acceptable Use Policy/Rules of Behavior policy document. The Director of Human Resources retains the signed acknowledgements.