# LINCS System Security Plan

# NIST SP 800-53 Revision 4

## AC: Access Control

### AC-1: Access Control Policy And Procedures

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

##### AWS

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

##### CivicActions

CivicActions has developed, documented and disseminated to personnel an access control 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 Access Control (AC) Policy. This document can be found in the CivicActions Compliance Docs 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. Access control policy and procedures are documented in the LINCS SSP. Access to LINCS Technology Project operational information or system resources is limited to only authorized users, programs or processes. The Department enforces access control policies to protect the integrity of the LINCS Technology Project system. This Department reviews and updates this policy as necessary and it has been being updated, as necessary, since April 2008. Additional information is contained within the Department of Education, OCIO-01, Handbook for Information Assurance Cybersecurity Policy.

### AC-2: Account Management

The organization: a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types]; b. Assigns account managers for information system accounts; c. Establishes conditions for group and role membership; d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts; f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]; g. Monitors the use of information system accounts; h. Notifies account managers: 1. When accounts are no longer required; 2. When users are terminated or transferred; and 3. When individual information system usage or need-to-know changes; i. Authorizes access to the information system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Other attributes as required by the organization or associated missions/business functions; j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

##### 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 account management.

#### a

##### CivicActions

CivicActions Operations, in collaboration with CivicActions Security, will set up privileged accounts accounts for the following roles:

• Developer - user level account that has access to application features and sanitized databases

• System Administrator - user accounts that enjoy full system administrator access

##### Drupal

Drupal provides user accounts for individuals who participate in visiting, contributing to and administering the site with the following roles:

• Anonymous user – readers of the site who either do not have an account or are not logged in.

• Authenticated user – All non-anonymous users inherit the “authenticated user role.”

• Administrator - This role has all permissions enabled by default.

##### LINCS

SSH system accounts are provided to contractors on an as-needed basis. Access privileges are used to ensure that only authorized personnel access certain areas of the LINCS Technology Project system. User access is controlled by the completion and submission of LINCS Technology Project System Rules of Behavior and New User Account Request forms by the user and management. These items are completed and submitted whenever a new user requires access or an existing user requires access changes. The system administrator, based on need-to-know, assigns the proper permissions. The employee’s manager approves the access rights before the initial account is created. Finally, the system administrator implements the access rights according to the New User Account Request form. The security staff and the support contractor review accounts periodically. Accounts no longer in use are removed from the system by the system administrator. The LINCS Technology Project has implemented user account procedures to disable inactive user accounts after 90-days of inactivity. The LINCS support staff monitors all user accounts to ensure this procedure is enforced. Section 6.3, Authentication Management, of the LINCS SSP illustrates the exact procedures the contractor support staff follows to ensure accounts are properly managed. The LINCS Technology Project system does not have guest or anonymous accounts.

#### b

##### CivicActions

CivicActions’ Project Manager assigns the “admininstrator” role for the management of all accounts issued to internal admin roles supporting the information system. Account requests are initiated by the Project Manager by completing a ticket request and the CivicActions Operation Team manages the entire account creation process.

##### LINCS

The System Owner has oversight over all permissions that the Project Manager and Operations Staff manages.

#### c

##### LINCS

In accordance with LINCS Access Control Policy, LINCS group membership is determined according to the individual’s position and role within the organization. A ticket request is used to request accounts and group membership. The request is authorized by the appropriate manager.

#### d

##### CivicActions

All accounts issued for application administrators and SSH are documented in CivicActions’ ticketing system. Account request tickets contain details that explain the attributes for the account including authorized users of Drupal, system infrastructure, group and role membership, and access authorizations.

##### Drupal

Drupal has a sophisticated permissions and role-based access control built in. Each role within Drupal can only access the documents and controls for which their privilege allows.

##### LINCS

LINCS user privileges vary depending on the type of user role assigned. Only users with the role of Administrator have the ability to create and modify user roles for other users.

#### e

##### CivicActions

All accounts issued for the admin management of Application or SSH access must be approved by the System Owner or Project Manager who must create an account request. The CivicActions Operations Team applies appropriate account permissions and settings based on the job role and function documented within the request ticket using processes defined by the CivicActions Security Team.

##### LINCS

The System Owner approves, and CivicActions Operations set up the initial Administrator account for LINCS. Subsequent client access and related approvals are managed by CivicActions Operations in collaboaration with the System Owner.

#### f

##### CivicActions

CivicActions Operations is responsible for the following account management activities for both internal administrative users and customer accounts: • Establishing account justification • Activating accounts • Modifying accounts • Expiring accounts • Disabling accounts • Removing accounts

#### g

##### CivicActions

All CivicActions systems log the usage of information accounts.

##### Drupal

Drupal monitors the usage of information accounts in the watchdog.log.

#### h

##### CivicActions

In accordance with the CivicActions Access Control (AC-01) Policy when an account is no longer required, the Project Manager notifies the Operations Team to immediately disable all access. Users upon reassignment, change in roles, termination, or leaving employment are initially removed from all roles and groups, effectively denying them all access to privileged accounts.

#### i

##### CivicActions

System accounts require access authorizations prior to accounts being created. The Project Manager must initiate an access request for an account to be created. CivicActions Operations reviews the request to ensure accuracy, including intended system usage and other attributes of the user access being requested.

##### LINCS

LINCS governs their own administrative access. Users with the Administrator roles are empowered to designate and approve Administrators.

#### j

##### CivicActions

All privileged accounts are reviewed by CivicActions Operations every 180 days.

##### LINCS

Administrators are empowered to and responsible for reviewing their own accounts and determining whether the accounts should still be authorized.

#### k

##### CivicActions

In accordance with standard security best practices and CivicActions policy, shared and reissued accounts for internal accounts of any kind are not created nor used for any purpose in any system.

### AC-3: Access Enforcement

The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

##### 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 account management.

##### Drupal

Access control in Drupal is enforced by authentication via unique username/password for every type of user except Anonymous user. The user’s privileges, permissions and access are provided on “least privilege” principle. The anonymous user role has the least access to the site of all roles. The website does not allow anonymous users to register an account for themselves. Drupal Administrators are the only user roles that can create new user accounts.

##### LINCS

The LINCS Technology Project ensures that assigned authorizations for controlling access to the system is enforced in accordance with the user definitions noted in Section 1.1.1 of the LINCS SSP. The technical support staff ensures that access to security functions and protected information is restricted to authorized personnel. Access will be controlled with access control list used on each instance. Members of one group cannot access resources defined for other groups unless explicitly permitted.

### AC-6: Least Privilege

The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

##### AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: application of least privilege.

##### CivicActions

CivicActions performs regular audits of privileged users as part of the practice of enforcing least privilege.

##### Drupal

CivicActions implements the policy of least privilege for all logical components of Drupal by allowing only authorized access for users, which are necessary to accomplish assigned tasks in accordance with business functions and organizational need. At the application layer, Drupal is designed with a role based user access system, a least privileged approach based on assignment of privileges to roles. Drupal‘s permission systems enables control of what users can do and see on the site. CivicActions has defined a specific set of permissions for each of the user roles mentioned in control AC-5. SSH access is provided on a least privilege basis and analyzed on an ongoing basis, at least quarterly. Findings related to these audits of accounts are reported and reviewed by the CivicActions Data team and evaluated to determine roles that need to be revoked.

##### LINCS

Drupal privileged access roles are designated by LINCS which is responsible for determining who will have administrator privileges and the ability to create other user accounts, including user accounts with the role of “administrator”.

### AC-6 (9): Auditing Use Of Privileged Functions

The information system audits the execution of privileged functions.

##### Drupal

CivicActions, at least quarterly, audits all team accounts based on the concept of least privilege. Each member of the developer team is assigned a role of which defines access needed to perform only the member’s job function. The audit of accounts is reported and reviewed by the CivicActions Operations and evaluated to determine whether roles or membership within the developer team should be changed.

### AC-7: Unsuccessful Logon Attempts

The information system: a. Enforces a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and b. Automatically [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next logon prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded.

##### AWS

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

##### LINCS

The LINCS Technology Project system locks out users after three unsuccessful login attempts. The information system automatically locks the account permanently, unless an administrator unlocks the account before then, when the maximum number of unsuccessful attempts (3) is exceeded.

#### a

##### Drupal

Drupal can be configured to lock an account after a specified number of invalid login attempts within specified time period.

#### b

##### Drupal

Lock down following unsuccessful attempts is configurable by Drupal administrators to conform to defined requirements. When a user exceeds the limit of invalid logon attempts, their account is automatically locked for a specfied time and requires administrator action to unlock the account before the lockout period expires.

### AC-8: System Use Notification

The information system: a. Displays to users [Assignment: organization-defined system use notification message or banner] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: 1. Users are accessing a U.S. Government information system; 2. Information system usage may be monitored, recorded, and subject to audit; 3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and 4. Use of the information system indicates consent to monitoring and recording; b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: 1. Displays system use information [Assignment: organization-defined conditions], before granting further access; 2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and 3. Includes a description of the authorized uses of the system.

##### LINCS

A warning banner ensures that all persons attempting to gain access to the system know that the system and its information are “Authorized User Only” and that attempts to illegally log on to the system could lead to criminal prosecution. The warning message displayed notifies unauthorized users that they have accessed a U.S. Government computer system and continued, unauthorized use can be punishable by fines or imprisonment. Each device logged into will display a system use notification message before the log in window is displayed. The system use notification banner will remain on the screen until the user takes an explicit action to log on to the device. The following is the notification banner displayed on all Department instances: “You are accessing a U.S. Federal Government computer system intended to be solely accessed by individual users expressly authorized to access the system by the U.S. Department of Education. Usage may be monitored, recorded, and/or subject to audit. For security purposes and in order to ensure that the system remains available to all expressly authorized users, the U.S. Department of Education monitors the system to identify unauthorized users. Anyone using this system expressly consents to such monitoring and recording. Unauthorized use of this information system is prohibited and subject to criminal and civil penalties. Except as expressly authorized by the U.S. Department of Education, unauthorized attempts to access, obtain, upload, modify, change, and/or delete information on this system are strictly prohibited and are subject to criminal prosecution under 18 U.S.C § 1030, and other applicable statutes, which may result in fines and imprisonment. For purposes of this system, unauthorized access includes, but is not limited to: • Any access by an employee or agent of a commercial entity, or other third party, who is not the individual user, for purposes of commercial advantage or private financial gain (regardless of whether the commercial entity or third party is providing a service to an authorized user of the system); and • Any access in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State. If system monitoring reveals information indicating possible criminal activity, such evidence may be provided to law enforcement personnel.”

### AC-14: Permitted Actions Without Identification Or Authentication

The organization: a. Identifies [Assignment: organization-defined user actions] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

##### Drupal

The anonymous user role has the least access to the site of all roles. The website does not allow anonymous users to register an account for themselves.

##### LINCS

The Department of Education allows the general public user to read the web pages, do searches on the resource database and to review online forum information without identification and authentication for the public web site. Program and Privilege users cannot access LINCS Technology Project system without identification or authentication.

### AC-17: Remote Access

The organization: a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorizes remote access to the information system prior to allowing such connections.

##### AWS

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

##### CivicActions

The CivicActions Access Control (AC) policy defines policy for remote usage restrictions. The Project Manager or System Owner may additionally provision users according to their Access Control policies.

##### LINCS

The LINCS Technology Project permits remote access for privileged functions to support operational needs. The technical staff documents, monitors, and controls all methods of remote access to the information system including remote access for privileged functions. Privileged user access is only permitted through the use of Secure Shell (SSH) where the user will authenticate to the device through this secure channel. Virtual Private Networking (VPN) is not enabled in any form within the LINCS accreditation boundary.

### AC-18: Wireless Access

The organization: a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and b. Authorizes wireless access to the information system prior to allowing such connections.

##### AWS

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

##### CivicActions

This control is not applicable. The system does not provide wireless access points.

### AC-19: Access Control For Mobile Devices

The organization: a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and b. Authorizes the connection of mobile devices to organizational information systems.

##### AWS

The system inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: mobile device restrictions.

##### CivicActions

This control is not applicable. The system does not maintain a facility in which mobile device access limitations are required.

### AC-20: Use Of External Information Systems

The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: a. Access the information system from external information systems; and b. Process, store, or transmit organization-controlled information using external information systems.

##### AWS

The system inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: use of external information systems.

##### CivicActions

This control is not applicable. The system does not connect with external information systems.

### AC-22: Publicly Accessible Content

The organization: a. Designates individuals authorized to post information onto a publicly accessible information system; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and d. Reviews the content on the publicly accessible information system for nonpublic information [Assignment: organization-defined frequency] and removes such information, if discovered.

#### a

##### LINCS

The Department of Education grants certain LINCS support staff members the authority to post publicly accessible content. These individuals must complete LINCS system security training before being granted access to the LINCS and before they can post publicly accessible content within the LINCS. Furthermore, each authorized individual must follow the procedures delineated within the “Using Drupal” Instruction to ensure they are following a verifiable procedure throughout the entire process. This covers the LINCS Discussion Lists administration areas, LINCS Quarterly Reporting and training tools, and Drupal Content Management systems. Public content is only edited via the Drupal Content Management System. All other content is only viewable by LINCS system users and protected by hardened access controls.

#### b

##### LINCS

It is the LINCS responsibility to train authorized LINCS individuals ensuring publicly accessible information does not contain nonpublic information.

#### c

##### LINCS

Authorized LINCS individuals review the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included. LINCS Program Users have been authorized for creation of publicly accessible content with publishing authority from an Administrator role. The publishing authority ensures the information being published does not contain nonpublic information.

#### d

##### LINCS

Authorized LINCS individuals review the content on the publicly accessible information system for nonpublic information at least every 365 days and removes such information.