# LINCS System Security Plan

# NIST SP 800-53 Revision 4

## AU: Audit and Accountability

### AU-1: Audit And Accountability Policy And Procedures

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

##### LINCS

The LINCS Technology Project maintains a record of system activity by application process and by user activity. Audit and accountability policy and procedures are documented within the LINCS SSP. Security software features are used to automatically generate and store security audit log records for use in monitoring security-related events on all multi-user systems. The Department reviews and updates this policy as necessary and it was last updated in April 2008. Additional information is contained within the Department of Education Handbook for Information Assurance Security policy (Handbook OCIO-01).

### AU-2: Audit Events

The organization: a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events]; b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event].

##### AWS

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

#### a

##### CivicActions

CivicActions’ Security Policy provides information about auditing and logging of CivicActions internal users and end-user activity on the servers and within the system application.

##### Drupal

Transaction logs are generated by the Apache web server, Drupal CMS, MySQL database and PHP page processing. Specifically, the following server, application, database and network device audit log events are captured: • Apache access log :: Contains a list of requests for your website that have bypassed Varnish. These requests include pages, theme files, and static media files. • Apache error log :: Records any Apache-level issues. The issues reported here are usually caused by general server issues, including capacity problems, .htaccess problems, and missing files. • Drupal page request log :: Records all Drupal page loads on your website. • Drupal watchdog log :: Records Drupal-related actions on your website. The watchdog log is recorded on your server if you have enabled the syslog module. • MySQL slow query log :: Contains a list of MySQL queries that have taken longer than one second to complete. • PHP error log :: Records any issues that occur during the PHP processing portion of a page load. Issues reported here are usually caused by a website’s code, configuration, or content.

#### b

##### CivicActions

Auditable events may change due to changes in the threat environment. CivicActions teams collaborate internally and also communicate with customers and partner organizations to identify and select auditable events. The teams that participate in this process are described in control SA-3(b).

##### Drupal

All security-related issues and events, including requests for server log analysis, are recorded in CivicActions’ JIRA tracking system.

#### c

##### Drupal

CivicActions has extensive experience and specialization as a host of websites that are built using the Drupal web hosting platform. Our list of auditable events is also informed by the experience and advice of Drupal’s security team, which receives security vulnerability reports and publishes security updates related to Drupal and the more than 1 million websites that use the Drupal platform. Should the need for additional logging become evident, we have the ability to do so by modifying the website’s source code to insert additional Drupal watchdog hooks.

#### d

##### Drupal

Information captured in the transaction logs includes, but is not limited to, the following auditable events: • Failed login attempts • Successful login attempts • User account deletions • User account blocking/unblocking • Changes in user role assignments • Unauthorized attempts to alter protected user fields • New user account creation • Password reset instructions mailed • User logins via one-time login link • User logouts • Content creation (datasets, resources and other content types) • Content modification • Content deletion • Content publishing • Content unpublishing • File uploads • Web page not found • Website configuration changes • System administration activities • Slow query logs. • PHP error logs: Captures any errors logged during execution of the PHP programming language.

### AU-3: Content Of Audit Records

The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

##### AWS

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

##### Drupal

The logs collected for Drupal sites include the following types of information: • IP number of the request originator • Timestamp • Request URL • HTTP status code returned • Username • Drupal watchdog message (if applicable) • Unique numerical ID of the content being modified (for content creation, modification and deletion events) When auditing a Drupal incident, CivicActions’ developers aggregate log sources from multiple servers into the Graylog dashboard so that all log entries for a single managed security incident can be analyzed in a single document. Log sources are sorted, filtered and reviewed. Application logs are maintained primarily for after-the-fact investigation of critical system or security events.

### AU-4: Audit Storage Capacity

The organization allocates audit record storage capacity in accordance with [Assignment: organization-defined audit record storage requirements].

##### AWS

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

##### CivicActions

CivicActions ensures adequate storage capability requirements listed in AU-11 for all events from the application, database, and hosting environment.

### AU-5: Response To Audit Processing Failures

The information system: a. Alerts [Assignment: organization-defined personnel or roles] in the event of an audit processing failure; and b. Takes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].

##### AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013: response to audit processing failures. In the event of low storage or other system issues affecting audit, the AWS CloudWatch monitoring system will alert CivicActions Operations via real-time alert mechanism such as OpsGenie.

##### CivicActions

When notified (e.g., via CloudWatch) of an auditing failure, CivicActions Operations will review the causes and take corrective action.

### AU-6: Audit Review, Analysis, And Reporting

The organization: a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity]; and b. Reports findings to [Assignment: organization-defined personnel or roles].

##### AWS

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

#### a

##### CivicActions

CivicActions security audit data is collected by a Graylog Security and Event Management (SIEM) dashboard to support real-time and after-the-fact investigation at the application level for the following: • Indications of inappropriate or unusual activity • Assurance that logging is functioning properly • Adherence to logging standards identified in this procedure

#### b

##### CivicActions

Any significant findings observed during the inspection are reported to CivicActions Security. If these are considered to constitute a security incident, then the Incident Response process is invoked as described in the implementation of the Incident Response Plan (IR-8).

### AU-8: Time Stamps

The information system: a. Uses internal system clocks to generate time stamps for audit records; and b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [Assignment: organization-defined granularity of time measurement].

##### AWS

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

##### LINCS

The LINCS Technology Project system clocks are synchronized system-wide and provide time stamps with audit records.

### AU-9: Protection Of Audit Information

The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

##### AWS

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

##### CivicActions

CivicActions ensures that audit logs are created, stored and maintained. Developers who have been assigned as members of the CivicActions Security Team are the only CivicActions personnel with logical permission to access and review audit logs.

### AU-11: Audit Record Retention

The organization retains audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

##### AWS

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

##### CivicActions

CivicActions audits events from the application, database, and hosting environment, and retains these records for at least 180 days.

### AU-12: Audit Generation

The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [Assignment: organization-defined information system components]; b. Allows [Assignment: organization-defined personnel or roles] to select which auditable events are to be audited by specific components of the information system; and c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.

##### AWS

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

#### a

##### CivicActions

CivicActions ensures audit records are generated for its web and event logs as required in AU-2 and AU-3 for servers, application, database and network components.

#### b

##### CivicActions

The selected auditable events described in AU-2 are coordinated by CivicActions internal admins and client security/operations officers for each component of the production system.

#### c

##### CivicActions

CivicActions maintained applications generate audit records for their web and event logs as described in AU-2 and AU-3.