# AUDIT AND ACCOUNTABILITY

## AU-01 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

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

Security control type: Hybrid

#### LINCS specific control or LINCS Responsibility

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).

#### CivicActions Responsibility

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>.

#### 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 Providers dated 1 May 2013.

## AU-02 AUDITABLE EVENTS

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

Security control type: Hybrid

#### 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 dated 1 May 2013.

### Part a)

#### CivicActions Responsibility

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 specific control support

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.

### Part b)

#### CivicActions Responsibility

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 specific control support

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

### Part c)

#### Drupal specific control support

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.

### Part d)

#### Drupal specific control support

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-03 CONTENT OF AUDIT RECORDS

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

Security control type: Hybrid

#### Drupal specific control support

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.

#### 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 dated 1 May 2013.

## AU-04 AUDIT STORAGE CAPACITY

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

Security control type: Inherited (Cloud Service Provider)

#### CivicActions Responsibility

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

#### 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 dated 1 May 2013 for the following: disk space availability.

## AU-05 RESPONSE TO AUDIT PROCESSING FAILURES

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

Security control type: Hybrid

#### CivicActions Responsibility

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

#### 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 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.

## AU-06 AUDIT REVIEW, ANALYSIS, AND REPORTING

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

Security control type: Hybrid

#### 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 dated 1 May 2013.

### Part a)

#### CivicActions Responsibility

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

### Part b)

#### CivicActions Responsibility

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-08 TIME STAMPS

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

Security control type: Hybrid

#### LINCS specific control or LINCS Responsibility

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

#### 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 dated 1 May 2013.

## AU-09 PROTECTION OF AUDIT INFORMATION

Control description: <http://800-53.govready.com/control?id=AU-9>

Security control type: Inherited (Cloud Service Provider)

#### CivicActions Responsibility

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.

#### Amazon Web Services (AWS) US-East/West control support

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

## AU-11 AUDIT RECORD RETENTION

Control description: <http://800-53.govready.com/control?id=AU-11>

Security control type: Inherited (Cloud Service Provider)

#### CivicActions Responsibility

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

#### 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 dated 1 May 2013.

## AU-12 AUDIT GENERATION

Control description: <http://800-53.govready.com/control?id=AU-12>

Security control type: Hybrid

#### 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 dated 1 May 2013.

### Part a)

#### CivicActions Responsibility

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.

### Part b)

#### CivicActions Responsibility

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.

### Part c)

#### CivicActions Responsibility

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