# LINCS System Security Plan

# NIST SP 800-53 Revision 4

## IR: Incident Response

### IR-1: Incident Response Policy And Procedures

The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and b. Reviews and updates the current: 1. Incident response policy [Assignment: organization-defined frequency]; and 2. Incident response 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 an incident response 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 Incident Response (IR) Policy and Procedure that 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. The LINCS Technology Project maintains an Incident Response Plan (IRP), consistent with Department of Education Directives and NIST 800-61, which addresses purpose, scope, roles, and responsibilities. The incident response procedures address any activity or occurrence that compromises the integrity of a system, denies access to or use of IT resources, and compromises the sensitivity of the information stored in, processed by or transmitted by a system. Additionally, the IRP includes procedures to respond to waste, fraud, misuse, or abuse of any departmental IT system, damage or loss of software or data contained in any system, Use of unlicensed (pirated) software products, discovery of hardware or software vulnerabilities The LINCS Incident Response Plan can be found in the CivicActions Github repository at <https://git.civicactions.net/lincs/compliance/blob/master/docs/security-irp.md> Additional information is contained within the Department of Education, Handbook for Information Assurance Security Policy (Handbook OCIO-01) and the Department of Education, Handbook for Information Security Incident Response and Reporting Procedures (Handbook OCIO-14).

### IR-2: Incident Response Training

The organization provides incident response training to information system users consistent with assigned roles and responsibilities: a. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility; 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 dated 1 May 2013 for the following: incident response training.

##### CivicActions

All CivicActions employees are required to participate in incident response training, as required by Incident Response Plan changes, and annually. The CivicActions Incident Response Plan (<https://civicactions-handbook.readthedocs.io/en/latest/09-security/incident-response-plan>) is the basis for the training and the incident response workflow created by the Security team. Upon a review of past incidents, the training is updated to ensure processes and workflows are updated.

##### LINCS

CivicActions Operations and users of the LINCS system with incident response responsibilities are required to participate in incident response training once the role is assumed within 10 days, as required by LINCS changes, and annually. The Incident Response Plan (<https://git.civicactions.net/lincs/compliance/blob/master/docs/security-irp.md>) is the basis for the training and the incident response workflow created by the Security team. Upon a review of past incidents, the training is updated to ensure processes and workflows are updated.

### IR-4: Incident Handling

The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.

##### AWS

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

##### LINCS

The LINCS Technology Project’s Computer Security Officer (CSO) handles all incidents for the LINCS Technology Project. The CSO is prepared to report all incidents to The Department Computer Incident Response Capability (EDCIRC) and United States Computer Emergency Readiness Team (US-CERT) as necessary. The LINCS Technology Project utilizes proven incident handling methodologies for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. The Department maintains a list of lessons learned from ongoing incident handling activities and uses those lessons to update the incident response procedures accordingly. Preparation activities includes all CivicActions and LINCS internal users are trained if their role includes incident response. Detection monitoring tools providing notification to incident response personnel for analysis and action. Containment, eradication and recovery activities include AWS and LAMP-stack inherited fixes and LINCS system administrators adjusting IP port blocking security groups and SELinux policies.

#### a

##### CivicActions

CivicActions has implemented an Incident Response Plan (<https://civicactions-handbook.readthedocs.io/en/latest/09-security/incident-response-plan>) that explains the process for incident handling, and discusses preparation, detection and analysis, containment, eradication, and recovery. Preparation activities includes all CivicActions team members are trained in incident response. Detection and monitoring tools providing notification to incident response personnel for analysis and action.

#### b

##### CivicActions

CivicActions Operations and Security team leads are members of the CivicActions Contingency and Incident Response Plan teams which coordinates activities accordingly through the life of the incident event.

#### c

##### CivicActions

CivicActions Operations and Security conduct a post-incident analysis to assist in documenting lessons learned and suggesting changes to improve the incident response process. Tickets created in response to the incident event are reviewed upon completion by Engineering and Security teams. Changes to the Incident Response Plan (<https://civicactions-handbook.readthedocs.io/en/latest/09-security/incident-response-plan>) require a team review session for approval.

### IR-5: Incident Monitoring

The organization tracks and documents information system security incidents.

##### AWS

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

##### CivicActions

CivicActions utilizes the JIRA ticketing tool for tracking and reporting of incident events from reporting to resolution and post-incident analysis. Initial reporting can come from continuous monitoring tools as well as client and public submissions made to support@civicactions.com. Jira processes the tickets for the public submissions and CivicActions’ Support Team creates associated GitHub Issues. Internal incidents reported are processed within the GitHub Issue queue. Details of the handling procedures are included in the CivicActions Incident Response Plan (<https://civicactions-handbook.readthedocs.io/en/latest/09-security/incident-response-plan/#response-process>) Response Process.

##### LINCS

The LINCS Technology project utilizes network and host-based intrusion detection systems, monitoring the system and application logs for anomalous events. Incidents are tracked using the same ticketing system that is used to track all system-related changes and events.

### IR-6: Incident Reporting

The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within [Assignment: organization-defined time period]; and b. Reports security incident information to [Assignment: organization-defined authorities].

##### AWS

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

##### LINCS

If an incident involves suspicious activity, CivicActions Operations will contact the LINCS System Owner who may then contact the LINCS CSO. The LINCS Technology Project’s Computer Security Officer (CSO) handles all incidents for the LINCS Technology Project. The CSO is prepared to report all incidents to The Department Computer Incident Response Capability (EDCIRC) and United States Computer Emergency Readiness Team (US-CERT) as necessary.

#### a

##### CivicActions

CivicActions personnel, as soon as an incident event is detected and/or communicated, are required to report the incident event to CivicActions Security. Methods of detection and/or communication may include one or more of: • Though continuous monitoring tools (StatusCake, OSSEC, others). • As a result of application notifications where CivicActions Security receives notifications (AIDE, OpsGenie, others). • Event logging described in AC-2 • Host based alerts from the cloud infrastructure or platform.

#### b

##### CivicActions

CivicActions personnel, as soon as the incident event is detected and/or communicated, are required to report the incident event to CivicActions Security.

### IR-7: Incident Response Assistance

The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

##### AWS

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

##### CivicActions

CivicActions HelpDesk team provides first response assistance to any users of the system. Response time for external reporting of incidents through e-mail is one business day. Internal users are able to request support thought the same process or initiate the incident response workflow. Tickets created in the Jira (customer ticketing system) and GitLab (internal ticketing system) documents all details related to the incident to assist the incident response teams in handling the incident.

### IR-8: Incident Response Plan

The organization: a. Develops an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and 8. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; b. Distributes copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; c. Reviews the incident response plan [Assignment: organization-defined frequency]; d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; e. Communicates incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and f. Protects the incident response 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: incident response plan.

##### LINCS

The LINCS Incident Response Plan (<https://git.civicactions.net/lincs/compliance/blob/master/docs/security-irp.md>) includes a comprehensive incident response program, which details the implementation of procedures and tools required for incident handling. The incident response program details the roles and responsibilities of LINCS/CivicActions IR Team. The IR Team includes members from CivicActions Security and Operations teams. Incident response plays a pivotal role in monitoring, detecting and handling security incidents of the entire information system. The IRP details categorization of incidents in accordance with NIST 800-61 and accordingly documents and reports incidents. The IRP is reviewed annually and updated as needed by ISSO, with the assistance of the incident response team.

#### a

##### CivicActions

Incident response plays a pivotal role in monitoring, detecting and handling security incidents of the entire information system. CivicActions has developed an Incident Response Plan (<https://civicactions-handbook.readthedocs.io/en/latest/09-security/incident-response-plan>) that: 1. provides CivicActions with procedures and tools required for incident handling; 2. describes the structure and organization of the incident response capability; 3. provides a high-level approach for how the incident response capability fits into CivicActions and the systems it maintains; 4. meets the mission, size, structure, and functions of CivicActions; 5. defines reportable incidents; 6. provides metrics for measuring the incident response capability and details categorization of incidents in accordance with NIST 800-61;

1. defines the roles and responsibilities of CivicActions IR Team;
2. is reviewed annually and updated as needed by CivicActions Security, with the assistance of the Incident Response team.

#### b

##### CivicActions

The CivicActions Incident Response Plan is distributed to all CivicActions team members as part of the CivicActions Handbook (<https://civicactions-handbook.readthedocs.io/en/latest/09-security/incident-response-plan>). The Incident Response team includes members from Security, Engineering, and Drupal Engineering teams.

#### c

##### CivicActions

CivicActions Security and the Incident Response team is responsible for reviewing the Incident Response Plan annually. The entire incident response team will review the plan and update it as necessary. Ultimately, the CISO has final say and will approve all updates to the plan.

#### d

##### CivicActions

CivicActions Security is responsible for managing the IR Plan, including annual reviews and updates. The IR Plan is updated to reflect any changes to processes, systems or applications. In addition, any concerns or difficulties encountered during IR Plan implementation, execution, or testing are addressed in an update to the IR Plan.

#### e

##### CivicActions

Modifications to the IR Plan are conducted by the IR team (CivicActions Security, Operations and Engineering teams) and communicated to the CivicActions team.

#### f

##### CivicActions

The IR Plan is available in the CivicActions Handbook and is maintained in the CivicActions Github repository. Github provides the configuration management capabilities for the IR Plan to be protected from unauthorized disclosure and modification.