# LINCS System Security Plan

# NIST SP 800-53 Revision 4

## CP: Contingency Planning

### CP-1: Contingency Planning Policy And Procedures

The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A contingency 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 contingency planning policy and associated contingency planning controls; and b. Reviews and updates the current: 1. Contingency planning policy [Assignment: organization-defined frequency]; and 2. Contingency 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 contingency 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 Contingency Planning (CP) 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 has developed a contingency planning policy consistent with Department of Education, Handbook for Information Technology Security Contingency Planning Procedures (Handbook OCIO-10) and NIST 800-34. Contingency planning procedures are formally documented within the LINCS Technology Project Contingency Plan, which provides the roles and responsibilities as it pertains to contingency planning. The Department reviews and updates the policy as necessary and the policy was last updated in July 2012.

### CP-2: Contingency Plan

The organization: a. Develops a contingency plan for the information system that: 1. Identifies essential missions and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and 6. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; b. Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the information system [Assignment: organization-defined frequency]; e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and g. Protects the contingency plan from unauthorized disclosure and modification.

#### a

##### AWS

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

##### CivicActions

CivicActions has developed a contingincy plan for that addresses: 1. Essential missions, business functions and associated contingency requirements 2. Recovery objectives, restoration priorities, and metrics 3. Roles and responsibilities are identified in the CP and includes the ISCP Director, Incident Commander (IC), CivicActions Coordinator, and CivicActions Information System Security Officer (ISSO). 4. Maintaining essential missions and business functions despite an information system disruption, compromise, or failure 5. Full information system restoration without deterioration of the security safeguards originally planned and implemented 6. The ISCP is reviewed and approved by ISCP Director, Incident Commander (IC), CivicActions ISSO and the System Owner annually.

#### b

##### CivicActions

The CivicActions Information System Contingency Plan (ISCP) has been distributed to all CivicActons team members. The ISCP can be found in the CivicActions Handbook at <https://civicactions-handbook.readthedocs.io/en/latest/09-security/contingency-plan/>.

##### LINCS

The LINCS Information System Contingency Plan (ISCP) has been distributed to all members who have roles in Contingency Planning and Incident Response team. Direction by the System Owner will update who is required to receive a copy of the contingency plan. The ISCP can be found in the LINCS GitHub wiki at <https://git.civicactions.net/lincs/compliance/blob/master/docs/contingency-plan.md>.

#### c

##### CivicActions

The Information System Contingency Plan (ISCP) is closely integrated with the Incident Response Plan (IRP). Coordination is the responsibility of the ISCP Director and CivicActions Operations.

#### d

##### CivicActions

The ISCP Director and CivicActions Security are responsible to review the ISCP annually and when a change to the system occurs.

#### e

##### CivicActions

CivicActions Operations and ISCP Director are required to update the ISCP to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing.

#### f

##### CivicActions

The ISCP requires that changes to the plan be communicated to those on the Incident Response / Contingency Plan Contact List.

#### g

##### CivicActions

The ISCP is available on CivicActions Github repository. This repository provides the configuration management capabilities for the ISCP to be protected from unauthorized disclosure and modification.

### CP-3: Contingency Training

The organization provides contingency training to information system users consistent with assigned roles and responsibilities: a. Within [Assignment: organization-defined time period] of assuming a contingency 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: contingency plan training.

##### CivicActions

The ISCP stipulates that all CivicActions system assigned roles in the Contingency Plan Team are trained in their duties within three months of first being assigned a role in the CP, and then annually thereafter or when changes are required. CivicActions uses the Contingency Plan as described in controls CP-1 and CP-2 as a basis for personnel contingency training.

### CP-4: Contingency Plan Testing

The organization: a. Tests the contingency plan for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the effectiveness of the plan and the organizational readiness to execute the plan; b. Reviews the contingency plan test results; and c. Initiates corrective actions, if needed.

##### AWS

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

##### CivicActions

Real world tests of the contingency plan will be held at least annually, with supplemental tests (checklist/table-top) as needed for specific scenarios. The ISCP Coordinator is responsible to facilitate annual testing exercises. The testing process for the ISCP includes review of the ISCP, exercise and identification of corrective actions and other improvements.

### CP-6: Alternate Storage Site

The organization: a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

##### AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: alternate storage site

### CP-6 (1): Separation From Primary Site

The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

##### AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: alternate storage site separation.

### CP-9: Information System Backup

The organization: a. Conducts backups of user-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; b. Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; c. Conducts backups of information system documentation including security-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and d. Protects the confidentiality, integrity, and availability of backup information at storage locations.

#### a

##### AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: user level backup requirements.

##### CivicActions

CivicActions conducts system user-level information backup in accordance with requirements (at a minimum, incremental backups must be conducted at least weekly and full backups must be conducted at least monthly).

#### b

##### AWS

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

##### CivicActions

System level information for the application is replicated and backed up in the same way as user-level information as defined in CP-9(a).

#### c

##### CivicActions

System documentation is backed up from the GitHub repository on a daily basis with a minimum two-week retention period and off-site storage.

#### d

##### AWS

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

##### CivicActions

CivicActions employees must authenticate prior to being granted access to the GitHub repository. Roles and responsibilities within GitHub determine the proper level of access for the documentation being accessed. The folder structure of GitHub protects though permissions and ownership prohibiting users from accessing unauthorized documentation.

### CP-10: Information System Recovery And Reconstitution

The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

##### AWS

The system partially inherits this control from the FedRAMP Provisional ATO granted to the AWS Cloud dated 1 May 2013 for the following: information system recovery and reconstitution.

##### CivicActions

The Contingency Plan documents the mechanisms with supporting procedures that allow all system components to be recovered and reconstituted to the system’s original state after a disruption or failure. This original state means that all system parameters (either default or organization-established) are reset, patches are reinstalled, system and security configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled, information from the most recent backups is available and the system is fully tested.