# Reusable Component Library 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].

**Status:** Partial

**Summary:** Partially inherited from AWS (FedRAMP).

##### 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>.

### 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.

**Status:** Partial

**Summary:** Partially inherited from AWS (FedRAMP).

#### a

##### CivicActions

CivicActions has developed a contingency 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 include 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 CivicActions team members. The ISCP can be found in the CivicActions Handbook at <https://civicactions-handbook.readthedocs.io/en/latest/09-security/contingency-plan>.

#### 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 staff.

#### d

##### CivicActions

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

#### e

##### CivicActions

CivicActions Operations staff 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.

**Status:** Partial

**Summary:** Partially inherited from AWS (FedRAMP).

##### 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.

**Status:** Partial

**Summary:** Partially inherited from AWS (FedRAMP).

##### 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 a review of the ISCP, exercise, and identification of corrective actions and other improvements.

### 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.

**Status:** Partial

**Summary:** Partially inherited from AWS (FedRAMP).

#### a

##### AWS

In this architecture, user data is limited to that which is stored in the Amazon RDS database. RDS is fully backed up by a daily snapshot as well as through transaction logging conducted by AWS as part of this managed service. Full database recovery from snapshot or point-in-time can be initiated from the RDS console/API.

##### 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

AWS built-in features automatically backs up system-level information limited to infrastructure CONFIGURATION information within the AWS account. While individual running EC2 instances and attached EBS volumes are NOT backed up, they can be reconstituted from Amazon Machine Images (AMIs) provided by AWS (which are backed up by AWS) and user data scripts included in CloudFormation templates. Once deployed, the CloudFormation template contents are backed up by AWS R488within the CloudFormation service. These AWS backups of AWS services are transparent to the customer as part of AWS backend processes.

##### 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

##### AWS

AWS built-in features back up online administrator and developer documentation, limited to that which is published at https://aws.amazon.com/documentation.

##### 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

AWS built-in features protect the confidentiality, integrity, and availability of information that AWS services back up. This information includes the service configuration information within an account, AWS online administrator and developer documentation, and AWS CloudFormation stacks for templates once deployed into an account. R612

##### 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.

**Status:** Partial

**Summary:** Partially inherited from AWS (FedRAMP).

##### 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.