# Project System Continuity Plan

## Client Project Full Name

March 2023 Version 3.4

CivicActions, Inc Lafayette, CA www.civicactions.com

2023 CivicActions, Inc All rights reserved.

Information contained in this document is proprietary, confidential, and intended for the use of CivicActions and the indicated client organization only.

* [1 Overview](#Xc8951b796c7b61cbdd4998c72efbdeed0056e13)
  + [1.1 Introduction](#X95cfb64b4e7a3c68f41b7aea44ce2e38e5bbf88)
  + [1.2 Plan Information](#X4e20649e28abfcfe579a9252453a72d97e6b15a)
* [2 Continuity of Operations Plan Overview](#Xef4a60da1687b3f44621d4dec74fea4bcc168f0)
  + [2.1 Applicable Provisions and Directives](#X6dd81d924204735b29d0568921d2864f5c1a2ed)
  + [2.2 Objectives](#X50548cef2869856644add0a3b227649964f3385)
  + [2.3 Organization](#Xd9641b2610e6457dc52d9b600d77e1e510646b4)
  + [2.4 Assumptions](#X8c2a7108f3f771461ab85188d04e234f9a4c755)
  + [2.5 Critical Success Factors and Issues](#X5ba602498ac86dc86440fd234597978ca81fc98)
  + [2.6 Mission-Critical Systems/Applications/Services](#Xa4deb9a3b8654ad8db6e08993ffa2c2ea61eb6e)
* [3 Continuity of Operations Plan](#Xea12d4b89e01cbe22e7b4e19336b25c8b42fbea)
  + [3.1 Plan Management](#X6dfd563a441906b9f57bfd32caeb5a2b25c81b1)
  + [3.2 Vital Records/Documentation](#Xf56c76350812a083f3c51fdc3b6d63ef15aa5f3)
* [4 Testing Procedures](#X716ed25f47f961d5302eef7bacbbddefbf7c457)
* [5 Recommended Strategies](#Xad7d1c9bba298e248b8e0f95a2283d337852226)
  + [5.1 Basic Emergency Response Procedures](#X321c9c65e65aa249f73a1c2cc5692174b5795c0)
  + [5.2 Diversification of Connectivity](#Xa48104d1fa9b0f7734714d153828a98568c9821)
* [6 Backup, Restore, and Recovery Procedures](#X8737093ae290eaab0f5ce993f7e4f1a941db40b)
  + [6.1 Backup Capabilities](#X04c564491b68dda7d371e80fd33d1f7aa4d6257)
  + [6.2 Backup Procedures](#X96bfe59c6589977d7fa3cc32f66e5a376d01678)
  + [6.3 Offsite Backup Procedures](#Xd78a9ac36dd2ef50fa5fa673bebdfd9101a05a5)
  + [6.4 Restore Procedures](#X6f339d7e06b14791b0d26bcc47b9a7bd2febf39)
  + [6.5 Contingency Log](#X85d00e2e37fe565b0c7750bbfad4a0c0310398b)
* [7 Continuity of Operations Plan Contact Information](#X4abce12ea4c67ba4dffb0795a9f3212403ed494)
  + [Contact List](#contact-list)

## 1 Overview

The Project facilitate collaboration between the communities the latest Enterprise 2.0 technologies, along with traditional communication tools will be used to ensure users can easily find and disseminate information between colleagues. The system is based on a content management system. The system is available to users over a traditional web interface using a desktop or laptop, but also through a mobile version of the web site accessible through mobile devices (phone and tablets). By enabling the latest collaboration techniques the Project will help the Client to fulfill their mission in a more efficient manner. System recovery time of 24 hours has been determined to provide a cost of recovery consummate with the value of the functionality provided by the Client. In light of this schedule, full system recovery can occur within the time frame, sparing the cost of a “hot” or “warm” site.

### 1.1 Introduction

The purpose of the System Continuity Plan (COOP) is to prepare for and address the elements necessary to sustain Project mission essential functions (MEF) at an alternate site and performing those functions for up to 30 days before returning to normal operations. Once a particular emergency is resolved, a synopsis of the problem and the resolution process in the form of a “lessons learned” document is generated and disseminated to all concerned. The COOP is intended to serve as the centralized repository for the information, tasks, and procedures that would be necessary to facilitate the Project management’s decision-making process and its timely response to any disruptive or extended interruption of normal business operations and services. This is especially important if the cause of the interruption is such that a prompt resumption of operations cannot be accomplished by employing only normal daily operating procedures. In terms of personnel and financial resources, the information tasks and procedures detailed in this plan represent Project management’s demonstrated commitment to response, resumption, recovery, and restoration planning.

### 1.2 Plan Information

The COOP is comprised of dynamic action plans to manage information system operational continuity objectives, and generally static policy that is managed by organizational processes. For Project, the majority of the COOP is contained in the action plan, which is captured in the [Project Contingency Plan](https://handbook.civicactions.com/en/latest/100-security/contingency-plan/) documentation.

## 2 Continuity of Operations Plan Overview

### 2.1 Applicable Provisions and Directives

The development of the Project COOP is required by both executive decision and regulatory mandates. The Project management must maintain an information assurance (IA) infrastructure that will ensure that its information resources maintain confidentiality, integrity and availability of its data and resources. Furthermore, Project management must ensure their strategic information resources management capabilities. Therefore, the Project COOP is developed in accordance with the following executive decisions, regulatory mandates, provisions, and directives as required by:

* Federal Information Security Management Act (FISMA 2002)
* Federal Information Security Modernization Act (FISMA 2014)
* Contingency Planning Guide for Federal Systems, NIST Special Publication 800-34r1 (May 2010)
* Risk Management Framework (RMF), NIST Special Publication 800-53r4 (April 2013)

### 2.2 Objectives

The primary focus of a COOP revolves around the protection of the two most important assets of any organization: personnel and data. The protection of personnel is inherited fully by the FedRAMP certification granted to the Amazon Web Services (AWS) cloud upon with the Project is built. Further, protection of data from fire, flood, power outages and other natural disasters is inherited through FedRAMP. Additional measures beyond the inherited capabilities are laid out in the Project Contingency Plan.

### 2.3 Organization

In the event of a disaster or other circumstances that may bring about the need for contingency operations, the normal organization of the Project will shift into that of the contingency organization. The focus the Project will shift from the current structure and function of “business as usual” to the structure and function of the Project working towards the resumption of time-sensitive business operations. The teams associated with the plan represent functions of a department or support functions developed to respond, resume, recover, or restore operations or facilities of the Project and its affected systems. Status and progress updates will be reported by each team leader to the plan owner. Close coordination must be maintained with the Project management and each of the teams throughout the resumption and recovery operations. The Project contingency organization’s primary duties are:: \* Protect information assets until normal business operations are resumed \* Ensure that a viable capability exists to respond to an incident \* Manage all response, resumption, recovery, and restoration activities \* Support and communicate with employees, system administrators, security officers, and managers

* Accomplish rapid and efficient resumption of time-sensitive business operations, technology, and functional support areas
* Ensure regulatory requirements are satisfied
* Exercise resumption and recovery expenditure decisions
* Streamline the reporting of resumption and recovery progress between the teams and management of each system

### 2.4 Assumptions

System recovery time of 24 hours has been determined to provide a cost of recovery consummate with the value of the functionality provided by Project. In light of this schedule, full system recovery can occur within the time frame, sparing the cost of a “hot” or “warm” site.

### 2.5 Critical Success Factors and Issues

This section addresses the factors and issues that specifically apply to the Project COOP that have been identified to be critical to its successful implementation. These factors are as follows: \* Commitment by upper management to Continuity of Operations Planning and Disaster Recovery.

* Budgetary commitment to Disaster Recovery.
* Modifications and improvements to the current scheduling procedures for the retention and transportation of backup files to the offsite storage facility.
* Development and execution of the necessary Memoranda of Agreement (MOAs), Memoranda of Understanding (MOUs), and Service Level Agreements (SLAs). ### 2.6 Mission-Critical Systems/Applications/Services

The following mission-critical systems/applications/services must be recovered at the time of disaster in the following order, due to interdependencies.

| System Identifier | System Description | Priority | Rationale |
| --- | --- | --- | --- |
| cpm | Backup management server (Cloud Protection Manager) | 1 | Expedites restore process |
| prod-db | the Project database | 2 | Required for the site to function |
| prod-web | the Project website | 2 | Required for the site to function |
| solr | the Project Search Server | 3 | Soft dependency for site search functions |
| staging | the Project Staging Server | 6 | For testing purposes only |
| dev | the Project Development Server | 6 | For development purposes only |

## 3 Continuity of Operations Plan

### 3.1 Plan Management

#### 3.1.1 Continuity of Operations Planning and Updates

The development of recovery strategies and work-arounds requires technical input, creativity, and pragmatism. The best way to create workable strategies and cohesive teams that leverage out-of-the-box thinking is to involve management and information resource management personnel in an ongoing, informative dialogue. The Project management has developed an agile Contingency Plan that is maintained in Git and regularly reviewed and updated by the development, operations and security teams.

#### 3.1.2 Continuity of Operations and System Contingency Team Members

The Project COOP, Contingency Plan and Security Incident Response team members are listed in the Project Incident Response Team Contact Details (private Google) spreadsheet which is linked to the Project Contingency Plan. Included are processes for: \* Incident Notification and Assessment \* Plan Activation \* Damage Assessment \* Remediation \* Disaster Recovery \* Retrospective (lessons learned)

### 3.2 Vital Records/Documentation

Vital records and important documentation are backed up and stored offsite and include any documents or documentation that is essential to the operations of an organization, such as personnel records, software documentation, legal documentation, legislative documentation, benefits documentation, etc. The following documentation will be available:

* Security related Information Technology (IT) policy & procedure memoranda, circulars, publications
* Complete hardware and software listings
* System testing plans/procedures
* System configuration
* Data backup/restoration procedures

## 4 Testing Procedures

The Project COOP will be maintained routinely and exercised/tested at least annually. Contingency procedures must be tested periodically to ensure the effectiveness of the plan. The scope, objective, and measurement criteria of each exercise will be determined and coordinated by the Project COOP Coordinator on a “per event” basis. The purpose of exercising and testing the plan is to continually refine resumption and recovery procedures to reduce the potential for failure. There are several different types of tests that are useful for measuring different objectives. The schedule for testing is as follows: \* Desktop testing on a quarterly basis \* One structured walk-through per year \* One integrated business operations/information systems exercise per year The COOP Coordinator, Contingency System Coordinators, and Team Leaders, together with the Project Management will determine end-user participation

## 5 Recommended Strategies

The following information represents potential strategies for execution and is considered as solutions that potentially may assist in the continued development of recovery capabilities in a post-disaster situation.

### 5.1 Basic Emergency Response Procedures

The actions set forth as responses to disasters are basic procedures that will be followed immediately prior to or during an actual contingency event. These procedures are designed to protect life; minimize damage, injury or disruption; and contribute to timely restart and recovery of the Project System.

#### 5.1.1 Procedures Inherited from the Cloud Service Provider (AWS) COOP

* Fire
* Water hazards
* Power failures
* Mechanical Failures
* Sabotage

### 5.2 Diversification of Connectivity

Amazon EC2 Region US-East is the primary the Project Cloud data center infrastructure with US-West as the secondary/contingency site. None

## 6 Backup, Restore, and Recovery Procedures

### 6.1 Backup Capabilities

All of the Project systems are dependent on the preservation of data, including software code and databases. In order to minimize the impact of a disaster, it is extremely important to protect the sensitivity or confidentiality of data; to preserve the authenticity and accuracy of data, and to maintain the availability of data. These three goals are commonly defined as “Confidentiality, Integrity, and Availability”. The protection of the confidentiality, integrity, and availability of data is of singular importance in information security and disaster recovery planning. Confidentiality, integrity, and availability of data are intrinsic to disaster recovery planning. For data backups, the system utilizes hourly encrypted snapshots of the file system, utilizing AWS elastic block storage (EBS) devices. A full set of these snapshot images is transferred daily to the secondary geographic location (US-West) for localized disaster recovery. The system also makes full logical backups of the primary the Project site database and stores them on virtualized storage.

#### 6.1.1 Hardware

Project inherits its hardware from the infrastructure COOP.

### 6.2 Backup Procedures

Backup procedures are vital to ensure that any interruption of service is minimized as far as is possible. Backup Log.

The backup schedule is as follows:

* Hourly snapshot backups of all operating system, application software and data. These are retained for 24 hours.
* Daily snapshot backups of all operating system, application software and data. These are retained for 30 days. Each backup is also transferred to the secondary geographic location (US-West).
* Daily full logical backups of the primary the Project site database. These are retained on filesystem for 6 days, with additional weekly backups retained for 35 days, and additional monthly backups retained for 150 days. The backup file system itself is also part of the daily snapshot backups and made available on the secondary geographic location (US-West). ### 6.3 Offsite Backup Procedures

See section 6.1.

### 6.4 Restore Procedures

There are three basic types of software recovery that must be anticipated, namely, data error recovery, hard disk recovery, and virus recovery. The guidelines for these procedures are as follows:

* Data Error Recovery – Use the last hourly backup. Overwrite the data with the contents of the backup, using the appropriate vendor software.
* Hard Disk Crash – Use the last hourly backup to re-install the system and application software.
* Virus – Once the start date of the virus has been determined, use the last weekly backup tape before that date to restore the system and application software.

In the event of serious infrastructure level incidents there are two scenarios:

* The first would be to use an alternate availability zone within the same US-East geographic region - in this case, the active disk volumes are already available and could just be attached to server instances in the alternate zone
  + in this instance, no backup snapshot is required, and the Elastic IPs can be instantly directed to the new servers.
* The second would be if the entire US-East region became unavailable (all availability zones). In this case we would bring up servers in the secondary US-West site, utilizing the most recent daily snapshots, and then update the domain name (DNS) entries to point to the new instance IPs.

### 6.5 Contingency Log

Assessments and results of any exercise or real contingency operations will be logged in JIRA from available documentation after recovery and restoration. Sections include lessons learned, unanticipated difficulties, staff participation, restoration of system backups, description of any permanently lost data, and shut down of temporary equipment used for the resumption, recovery, and restoration.

## 7 Continuity of Operations Plan Contact Information

This section includes all points of contact of positions described in the Continuity of Operations Plan (COOP) and key organizational personnel and contact numbers. the Project incident notification and system and network personnel are available 24x7.

### Contact List

To maintain current and accurate contact information, the contact list is maintained as a [private spreadsheet](None) and linked to the the Project Contingency Plan. If you require access to the source document, contact the ISO.