# Project Contingency Plan

## Contents

* [Overview](#overview)
  + [Preparedness](#preparedness)
  + [Plan maintenance](#plan-maintenance)
  + [Recovery objective](#recovery-objective)
* [Incident Response Team information Contact information](#X47c318437148f71b5224d2a5e240b2261b63bef)
* [Contingency plan outline](#contingency-plan-outline)
  + [Activation and notification](#activation-and-notification)
* [Recovery](#recovery)
  + [Backup and restore](#backup-and-restore)
  + [Reconstitution](#reconstitution)
* [External dependencies](#external-dependencies)
  + [GitLab](#gitlab)
  + [StatusCake](#statuscake)
  + [OpsGenie](#opsgenie)
  + [Jira](#jira)
  + [Slack](#slack)
  + [AWS](#aws)

## Overview

This Contingency Plan provides guidance for the CivicActions Team on delivering our essential mission and business functions following a disruption, compromise, or failure of any Project component.

“Disruption” means unexpected downtime or significantly reduced service lasting longer than:

* 30 minutes during standard U.S. business hours (0900-2100 EST, Monday through Friday)
* 90 minutes at other times

Disruption can include unexpected downtime of key services, data loss, or improper privilege escalation. In many cases, the robust contingency management capabilities of [AWS Cloud Security](https://aws.amazon.com/security/) coupled with [N2WS CPM backups and disaster recovery](https://n2ws.com/product/aws-disaster-recovery) will resolve/remediate event occurrences.

For a security incident and most events, the [Security Incident Response Plan](security-irp.md) provides guidance for the responding team.

### Preparedness

This plan is most effective if all core CivicActions team members know about it, remember that it exists, have opportunities to give input based on their expertise, and keep it up to date.

### Plan maintenance

The CivicActions team is responsible for maintaining and updating this document as needed. Changes must be approved and peer reviewed by another team member.

* All changes should be communicated to the team.
* Annually, and after major changes to our systems, we review and update the plan.

The CivicActions team protects this plan from unauthorized modification. This plan is stored in the CivicActions GitLab repository (https://guidebook.civicactions.com/en/latest/common-practices-tools/security/incidents/). Authorization to modify it is limited to the Incident Response Team by GitLab access controls. Per CivicActions policy, a team member proposes changes by making a pull request and asking another team member to review and merge the pull request.

### Recovery objective

Our objective is to recover from any significant problem (disruption, compromise, or failure) within 3 hours. Any disruption to Project services lasting more than 3 hours during standard U.S. business hours (0900 - 2100 Eastern Time) is considered unacceptable.

Short-term disruptions lasting less than 30 minutes are outside the scope of this plan.

## Incident Response Team information Contact information

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

## Contingency plan outline

### Activation and notification

The first Incident Response Team member who notices or reports a potential contingency-plan-level problem becomes the **Incident Commander** (IC) until recovery efforts are complete, or until the Incident Commander role is explicitly reassigned.

If the problem is identified as part of a [security incident response situation](security-irp.md) (or becomes a security incident response situation), the same Incident Commander (IC) should handle the overall situation since these response processes must be coordinated.

The IC first notifies and coordinates with the people who are authorized to decide that Project is in a contingency plan situation:

* From CivicActions:
  + Incident Commander
  + Project Manager
  + CivicActions Incident Response Team
* Project
  + Product Owner
  + Project users, when applicable

The IC keeps a log of the situation in a JIRA Incident ticket; if this is also a security incident, the IC also follows the [security incident communications process](security-irp.md#initiate) which includes updating the CivicActions Slack channel None Slack channel. The IC should delegate assistant ICs for aspects of the situation as necessary.

## Recovery

The Incident Response Team assesses the situation and works to recover the system. See the list of [external dependencies](#external-dependencies) for procedures for recovery from problems with external services.

If this is also a security incident, the IC also follows the [security incident assessment](security-irp.md#assess) and [remediation](security-irp.md#remediate) processes.

If the IC assesses that the overall response process is likely to last longer than 3 hours, the IC should organize shifts so that each responder works on response for no longer than 3 hours at a time, including handing off their own responsibility to a new IC after 3 hours.

### Backup and restore

Hourly and daily [snapshots](https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#Snapshots) are created using the [Cloud Protection Manager (CPM) or other backup system](https://cpm.project.com/signin/)

* First determine how far back in time to go to obtain a clean backup for restore
* Restore by using the Recover tab for the instance needing restoration

#### To recover a downed server

Note: *Volumes should not be deleted by default. If you terminate the old instance before you begin, CPM will attempt the re-use the internal “backnet” (172.x.x.x) addresses*

1. Log in to CPM at: <https://cpm.project.com/signin/>
   * Determine how far back in time to go to obtain a clean backup for restore.
   * Click **Recover** on the most recent hourly snapshots previous to issue occurrence.
   * Click **Instance** of the instance to be recovered.
   * Click **Recover Instance**.
2. Reset: *(this part needs additional documentation)*
   * Elastic IPs
   * Internal backnet addresses (in .ssh/config files) *(unnecessary if backnet preserved)*
   * System name tags of instances and volumes
   * Monitoring alarms *(if they had been disabled)*

#### Disaster recovery (DR)

Go to <https://n2ws.com/support/documentation/10-disaster-recovery-dr> and review the following sections:

* Performing DR on the N2WS Server (The cpmdata Policy)
* DR Recovery
* DR Instance Recovery
* DR of Encrypted Volumes, AMIs and Amazon RDS Instances

### Reconstitution

For reconstitution:

1. The Incident Response Team tests and validates the system as operational.
2. The IC declares that recovery efforts are complete and notifies all relevant people.
3. The IC schedules a postmortem in the JIRA ticket to discuss the event. This is the same as the [security incident retrospective process](security-irp.md#retrospective).

## External dependencies

Project depends on several external services. In the event one or more of these services has a long-term disruption, the team will mitigate impact by following this plan.

### GitLab

* **Service:** <https://gitlab.com>
* **Status:** <https://status.gitlab.com/>

If GitLab becomes unavailable, the Project will continue to operate in its current state. The disruption would only impact the team’s ability to update code on the instances.

### StatusCake

* **Service:** <https://app.statuscake.com/>
* **Status:** <https://twitter.com/StatusCakeTeam>

If there is a disruption in the StatusCake service, the Incident Response team will be notified by email.

### OpsGenie

* **Service:** <https://app.opsgenie.com/alert/>
* **Status:** <https://status.opsgenie.com/>
* **Status:** <https://twitter.com/opsgenie>

If there is a disruption in the OpsGenie service, all alerts automatically get delivered to the team via email.

### Jira

* **Service:** <https://project.atlassian.net/>
* **Status:** <https://twitter.com/JIRA>

None

### Slack

* **Service:** <https://slack.com/>
* **Status:** <https://status.slack.com/>
* **Status:** <https://twitter.com/SlackStatus>
* **Backup:** <https://chat.google.com/>

None

### AWS

* **Service:** <https://signin.aws.amazon.com/console>
* **Status:** <http://status.aws.amazon.com/>

If needed, you can [manage and create new servers](https://console.aws.amazon.com/ec2/v2/home).

In case of a **significant** disruption, after receiving approval from our Authorizing Official, the Contractor’s team will deploy a new instance of the entire system to a different region.