



Business Continuity and Disaster Recovery Plan

B:Hive Building, Smales Farm, 74 Taharoto Road, Takapuna, Auckland, 0622, New Zealand

WWW.FUEL50.COM | ENGAGE@FUEL50.COM | +64 9 356 9758



Summary

Overview

The Fuel50 Business Continuity Plan ("BCP") and Disaster Recovery Plan ("DRP") establishes procedures to recover Fuel50 operations following a disruption resulting from a disaster. The types of disasters contemplated by this plan include:

- natural disasters
- political disturbances
- man-made disasters
- external human threats
- and internal malicious activities.

Client facing Issues with functionality of the Fuel50 CareerDrive platform are described in the Fuel50 Incident Management Plan.

Disaster Recovery Policies

- Fuel50 performs testing of the Disaster Recovery Plan annually. The Platforms team is responsible for coordinating and conducting rehearsals of this Disaster Recovery Plan annually.
- Whenever the BCP/DRP is used, it must be followed by a retrospective and table-top re-enactment in order to identify lessons learned and playbooks needing creation.
- This plan must be updated at least annually with additional playbooks taking into account new risks of disasters learned through testing and re-enactment of past disaster incidents.

Scope

This plan includes all resources and processes necessary for service and data recovery, and covers all information security aspects of business continuity management. The following conditions must be met for this plan to be viable:

1. All equipment, software and data (or their backups/failovers) are available in some manner.
2. If an incident takes place at the organization's physical location, all resources involved in recovery efforts are able to be transferred to an alternate work site (such as their home office) to complete their duties.

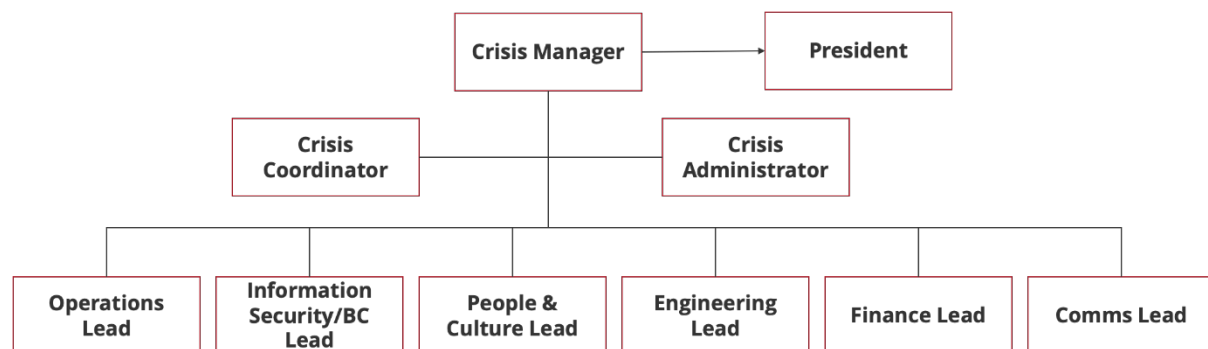
This plan does not cover the following types of incidents:

1. Incidents that affect customers or partners but have no effect on Fuel50's systems. In this case, the customer must employ their own continuity processes to make sure that they can continue to interact with Fuel50 systems.

- Incidents that affect cloud infrastructure suppliers at the core infrastructure level, including but not limited to Google, Slack, and AWS. Fuel50 depends on such suppliers to employ their own continuity processes.

Crisis Management Team Structure

The structure of the Crisis Management Team is shown below. Dependent on the particular Crisis the Crisis Manager will determine the roles that are required and other roles will be stood down. Should these roles be required at a later time they can always be recalled



Objectives

The objectives of this plan are the following:

- Enable existing or potential crises to be recognised promptly, and
- Identify the activities, resources, and procedures needed to carry out Fuel50's processing requirements during prolonged interruptions to normal operations.
- Identify and define the impact of interruptions to Fuel50's systems.
- Assign responsibilities to designated personnel and provide guidance for recovering Fuel50 operations during prolonged periods of interruption to normal operations.
- Ensure coordination with other Fuel50 staff who will participate in the contingency planning strategies.
- Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.
- Ensure crises are well managed, providing the best possible outcomes for the organisation and our stakeholders.

Defining Critical Systems and Services

From a disaster recovery perspective, Fuel50 defines two categories of systems:

Category 1 - Non-Critical Systems

These are all systems not considered critical by the definition below. These systems, while they may affect the performance and overall security of Critical Systems, do not prevent Critical Systems from functioning and being accessed appropriately. Non-Critical Systems are restored



at a lower priority than Critical Systems. Examples of Non-Critical Systems include analytics servers.

Category 2 - Critical Systems

These systems host application servers and database servers or are required for the functioning of systems that host application servers and database servers. These systems, if unavailable, affect the integrity of data and must be restored, or have a process begun to restore them, immediately upon becoming unavailable. The following services and technologies are considered to be critical for Fuel50 business operations, and must immediately be restored (in priority order):

1. Production infrastructure
2. Transit infrastructure
3. Build and deployment infrastructure

General Disaster Recovery Plan

While specific playbooks are available for specific scenarios, there are overall rules of engagement whenever a disaster incident needs to be opened.

Notification Phase

This phase addresses the initial actions taken to detect and assess damage indicted by a disruption to Fuel50. The notification sequence is listed below:

1. The first person to report the disaster should notify the Head of Engineering.
2. The GSPM is to notify team members referenced above in the crisis team.
3. Based on the damage assessment, if Fuel50 will be unavailable to customers for more than 6 hours the Head of Engineering will declare that a disaster has occurred and that the Disaster Recovery Procedure has been activated. The Head of Engineering also has the discretion to activate the Disaster Recovery Procedure based on other criteria.
4. In the event customer data has been compromised, customers must be notified no later than 24 hours after the incident is reported.
5. Once the Disaster Recovery Procedure has been activated, the Head of Engineering should notify relevant personnel and executive leadership on the general status of the incident. Notification can be conducted over chat, email or phone. The Head of Engineering may also notify the Fuel50 operations team if the disaster involves the Fuel50 premises or is related to Fuel50 employees.
6. If the Disaster Recovery Procedure has not been activated, the Recovery and Reconstitution phases will not be performed. Instead, the Head of Engineering and necessary team members will perform all appropriate tasks under Fuel50's Incident Response Plan.



7. Either the Head of Engineering or someone he or she selects will document who was contacted and when, and will summarise each call.

Recovery Phase

This phase covers the recovery of the application at an alternate site. If the disaster involves both Critical Systems and Non-Critical Systems, the Fuel50 Security team may prioritize the recovery of Critical Systems and proceed to the Reconstitution Phase for the Critical Systems before Non-Critical Systems have completed the Recovery Phase. This phase consists of the following tasks, some of which can be run in parallel:

1. Assess damage to affected environments, prioritizing critical systems first. Document observations.
2. If possible, back up the affected environments in a forensically sound manner. Do not alter affected systems and applications in any manner.
3. Verify that previous backups of critical databases and systems recovery points are available before moving on to the Reconstitution Phase.

Reconstitution Phase

This phase consists of activities necessary for restoring Fuel50 operations to the original operating state (or permanently move operations to the new site or state, if necessary). If the disaster involves both Critical Systems and Non-Critical Systems, the Fuel50 Platforms team may prioritize reconstituting the Critical Systems before beginning reconstitution of the Non-Critical Systems. This phase consists of the following tasks, some of which can be run in parallel:

1. Set up new AWS Account [if required]
2. Begin building AMI images in a new AWS Region [if required]
3. Begin building infrastructure from source control, using Terraform in failover AWS Region [if required]
4. Begin replication of new environment using previously confirmed backups using automated and previously tested scripts.
5. Fuel50 utilizes multiple availability zones; however, if the primary region is unavailable replicated backups should be used to create a production environment in the failover region.
6. Test logging, security and alerting functionality.
7. Deploy new environment to production.
8. Update DNS to new environment.

Note: Bitbucket repo, AWS account, working laptop with Terraform client, and access to the backup account where the data lives are required.

Forensics Phase

This phase consists of activities related to finding out the cause of the disaster, in cases where it is not immediately apparent. Upon the disaster incident being addressed, with customer data and Fuel50 operating infrastructure recovered and restored, it is appropriate to start the Forensics Phase. This phase consists of the following tasks, some of which can be run in parallel:

1. Ensure all logs from all systems, applications and databases involved in the incident have maintained their integrity in the centralized log repository.
2. If some logs did not reach the central log repository, ensure that missing system, database and application logs are retrieved. Pay attention to time keeping and clock settings, so logs from different sources can be reconciled.
3. If applicable, transfer data to a log analyser or test instance.
4. Target network, system, and user action logs for analysis. Analyse all logs manually or with tools, tests, and scripts that have already been previously tested.
5. Document all significant findings in the timeline.

Retrospective Phase

A retrospective of an event such as a disaster recovery incident allows for all parties to understand what happened in a clear and blame-free manner. A retrospective meeting should occur after such an incident has occurred.

1. All relevant parties and system owners should be identified and invited to a retrospective meeting.
2. A draft agenda and disaster timeline should be sent to everyone before the retrospective meeting.
3. Retrospectives are best facilitated with an unbiased third party who was not involved with working the incident. The facilitator should ask questions of meeting participants to illuminate the severity, impact, and any follow-ups.
4. Document the retrospective meeting.
5. Produce an incident report from the retrospective agenda, timeline, and meeting notes.

Re-enactment / Test Phase

Unanticipated disasters are unlikely to have documented steps for resolution. Once an unanticipated incident concludes, it should be re-enacted to analyse and document how to better respond in the future. If applicable:

1. Run a simulation of the event, as understood by the retrospective meeting notes, timeline, and report. The simulation can be run with people involved or uninvolved with the disaster.
2. While running the simulation, a pre-assigned note taker should write down ideas to prevent and mitigate a similar event.



3. After the re-enactment, a new and specific disaster recovery procedure should be created.

Reviewing and evaluation

The GSPM is responsible for reviewing this page at least every 12 months, and for updating it as necessary. The GSPM will notify all relevant interested parties upon each update.

Monitoring and Measurement

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- The page has been reviewed within period

Previous versions of this page must be stored for a period of 7 years unless specified otherwise by legal or contractual requirements.

Version Control

Date	Version	Person	Description of change
Aug 6, 2021	0.1	GSPM	Initial document template created
May 13, 2022	1.0	Platform Manager	First version approved
Jun 16, 2023	2.0	Platform Manager	Annual review. Minor changes applied
Jan 19, 2024	3.0	GSPM	Updated notification list
Mar 27, 2025	4.0	GSPM	Annual review. Minor changes applied