Uplevel Business Continuity Plan
Responsible Party: Albert Strong

Table of Contents

Purpose and Objectives

The objective of this Business Continuity Plan (BCP) is to provide guidance to Uplevel management for the restoration of facilities and critical business processes. It is an essential requirement that Uplevel provide ongoing supply of customer services to an acceptable level. The BCP defines, at a high level, the recovery procedures required to continue/restore core services in the event of a disaster.

This plan describes the organizational framework and procedures to be activated in the event of a disaster occurring, to enable recovery of services provided to Uplevel customers, including the public, and the relevant business units supporting these services.

Assumptions

The Uplevel BCP, is based on several assumptions that are critical to the proper execution and deployment of this plan. These assumptions must be taken into consideration when recovering operations at the cloud provider.

The following assumptions have been made regarding implementing this BCP:

- An event at a single affected cloud provider has occurred, and all other Uplevel services are operational
- The event is specific to the operations at the AWS location and has not impacted other relevant businesses
- Key internal contacts or alternate contacts are available to coordinate the recovery process

Scope

This plan is confined to the system operations and main business processes of Uplevel, Inc.

Pre-arranged Business Continuity Site

Uplevel has designed its corporate structure to be cloud based and independent from a traditional physical office building workplace. Consequently, Uplevel policy allows for employees and contractors to work remotely which in most cases means from home. Currently under this architecture there is no need for a contingency site.

Contingency Strategy

The contingency strategy aims to recover operations with minimal, if any, impact on the services supplied to our customers. The contingency strategy focuses on resolving issues relating to information technology, suppliers and service factors for services offered to Uplevel, Inc.'s customers and, where appropriate, the public.

Specifically, the contingency strategy focuses on:

- Immediate welfare of staff employed at the service site
- Assessing the workload requirements for each function
- Establishing priorities for, and allocate the use of, technological and human resources
- Delegating responsibilities for critical recovery procedures of each functional service area
- Central control of recovering operations

- Communicating the status of the event to customer representatives, management and alternate sites.

Equipment

Uplevel primarily operates in cloud environments. This enables operations to be recovered with minimal equipment such as a laptop and an Internet connection. There is an asset register of both internal and external equipment used in Uplevel services, and for all information assets across the Uplevel environment.

Buildings and Facilities

Uplevel primarily relies on cloud providers such as Amazon Web Services for systems operations. Testing and maintenance of emergency equipment i.e. fire alarms, extinguishers and emergency equipment is routinely conducted and managed by cloud service providers engaged by Uplevel.

Finance

Uplevel has comprehensive business insurance covering applicable assets.

Premise of the Plan

After performing a Business Impact Analysis (BIA), the business-critical activities, and the time frames within which they must be restored were identified.

The times below are indicative of the time taken to recover the relevant business critical activities. Recovery team members may use the table below as a reference when coordinating the continuity activities.

Summary of recovery period for Business Critical Functions

Business Critical Activities	Recovery Period
Office Space – not critical to restoring SaaS services	12 months
Cloud Services (Data, Technology & Communications)	24-48 hours
People, workforce, skills and knowledge	6 months
Finance – Revenue	12 months

Recovery Team Structure

The recovery team structure is critical to the success of the recovery process. The recovery team structure at Uplevel consists of a combination from each of the core functions.

The defined recovery structure enables recovery of organizational operations and manufacturing in a short period of time. Communication channels are essential to ensure that information flows throughout the organization, maximising the effort towards continuing service delivery to customers.

An overview of the recovery team structure for Uplevel indicated below:

Key roles and responsibilities are as follows:

Role	Name	Contact details

Office Space Recovery	Joe Levy	joe@uplevelteam.com
Cloud Service recovery	Dave Matthews	dave@uplevelteam.com
Application Recovery	Dave Matthews	dave@uplevelteam.com
People/Workforce Recovery	Joe Levy or Nimrod Vered	joe@uplevelteam.com, ravs@uplevelteam.com

Classifying the Event

Different disaster situations impact the business operations at Uplevel in unique ways. This BCP focuses on disaster scenarios that have a likelihood of occurring and highest impact on the operational performance of supplied customer services.

Disaster Scenarios

The circumstances which impact the operations of the Uplevel site have been identified to include disruptions resulting from natural, environmental and/or threatening events and include:

Natural
- Fire
- Flooding
- Pandemic
- Tornadoes and storms

Environmental
- Power/Utility failures
- Explosions
- Industrial Action
- External suppliers/Supply of service materials
- Equipment destruction/breakdown
- Cloud/IT malfunction
- Occupational Death

Threatening
- Sabotage by external parties (i.e. arson/vandalism)
- Bomb threats
- Security breaches

Potential Impacts

The service operations that might be impacted by the above disaster scenarios are as follows:

1. Loss of cloud facilities
2. Loss of IT systems/instances
3. Loss of key suppliers/cloud services providers

Impacts that are not identified above but may eventuate, such as staffing issues, will be resolved through routine management activities for recovery of manufacturing operations. Although an event may impact multiple service operations, the following table identifies the links between potential event and disaster scenarios.

Loss of facilities/cloud environment

This scenario impacts Uplevel Inc.'s ability to operate for a period of time. This scenario assumes that:

- There is complete loss of access to cloud services.
- The loss of service facilities is specific to Uplevel, Inc.'s operating region.

Loss of personnel

This scenario impacts Uplevel, Inc.'s from the effects of staff unavailability and assumes:

- Loss of key skills and knowledge
- Loss of senior management
- Loss of finance control and payroll

Loss of IT systems/Cloud instances

This scenario covers a total loss of IT infrastructure and assumes:

- Loss of network connectivity
- Loss of virtual server instances

Loss of Utilities

This scenario covers a total loss of utilities:

- Electricity
- Water
- Gas

Fast Action Summary Checklist

The initial response procedures are critical to efficiently managing a disaster scenario and reducing the impact on business operations at Uplevel The following key tasks are required to be completed and are used as the trigger for the initial response to the relevant disaster scenario. The following table acts as a checklist to ensure all relevant activities have been performed within the required time frames.

Ref	**Activity**	**Responsibility**	**Required time frame**
1	Notify Leadership Team of the incident including: ● Time of incident ● Manner in which incident was identified	All	Immediate upon identification of incident
2	Conduct initial assessment of incident and determine response	Leadership Team	1 – 15 minutes of incident notification
3	Notify First Aid/Appointed Person of incident to ensure adequate attention is provided to employees impacted by event	N/A	

4	Notify systems supplier (if loss of facilities is the incident)	Ravs / Dave	15 – 60 minutes of incident notification
5	Notify recovery team members of severity	Ravs / Dave	15 - 60 minutes of incident notification
6	Assess the need to instigate Uplevel Business Continuity Plan (BCP)	Leadership Team	15 - 120 minutes of incident notification
7	Announce activation of the BCP to all functional heads impacted by event	Leadership Team	15 - 120 minutes of incident notification
8	Convene the recovery team to determine: ● Frequency of meetings ● Resource requirements ● Service recovery processes Customer services impacted	Ravs / Dave	30 - 120 minutes of incident notification
9	Determine if the incident is likely to publicly impact Uplevel, Inc.	Leadership Team (Jori)	45 - 180 minutes of incident notification
10	Assess the need to release a communications briefing and release as determined appropriate	Jori	60 - 180 minutes of incident notification
11	Monitor and review the detailed recovery procedures relevant to the service and scenario	Leadership Team	Continuously

Recovery Timeframes

Timeframe
The timing of recovery activities is critical to ensure Uplevel, Inc.'s is able to recover operations with minimal impact to customer services. Each function is required to address key concerns at different times of a disaster event occurring. The timeframes considered critical to Uplevel, Inc.'s include:

- Period 1: immediate
- Period 2: 24 hours
- Period 3: 3 days
- Period 4: 7 days
- Period 5: 2-4 weeks

The above recovery periods are indicative of the critical business activities identified by management and relate to good recovery practices. Significant effort is often required for recovery of operations within the first 3 periods to ensure that minimal interruption/disruption to customer services exists.

The objectives of each recovery period are outlined below and need to be considered in developing and implementing recovery plans.

Period	**Objectives**
3	● Information sharing with staff ● Obtaining emergency services as appropriate
4	● Information sharing with key customers and suppliers ● Ensure IT/cloud provider has full backup of server ● Inform insurer

4	● Confirm cash flow status ● Evaluation of existing supplies and components completed
4	● Salvage activities completed ● IT hardware/cloud instances and software available
4	● Have staff located in temporary premises ● Production restart ● Facilities rebuilding

Recovery Procedures

Loss of Personnel

The following high-level recovery procedures are required to be completed when there is loss of 25% or more of Uplevel, Inc.'s staff or two or more critical functions due e.g. to a pandemic.

Period	Task Requirement
1	● Establish if temporary or permanent loss of personnel ● Assess medical or equivalent cause of loss
2	● Inform appropriate health authorities
4	● Arrange temporary staffing
4	● Complete initial training
5	● Quality competency check and training fully verified

Loss of IT/Cloud Provider

The following high-level recovery procedures are required to be completed when there is a computer system/communications failure e.g. to breakdown of server or telecom services.

Period	Task Requirement
2	● Contact CTO
2	● Obtain backup data
3	● Sanction replacement/virtual equipment
4	● Replacement systems fully functioning
4	● Data/systems will be obtained from alternative supplier (if necessary)

Loss of Key Suppliers/Cloud Services

The following high-level recovery procedures are required to be completed when there is a loss of one or more key suppliers.

Period	Task Requirement
3	● Contact supplier ● Establish if temporary or permanent ● Confirm related stock levels

4	● Contact second source
5	● Approach alternative sources of supply
5	● Alternative supplier auditing completed

Testing and Maintenance Procedures

Testing and maintenance of the BCP is critical to ensuring that the document remains both relevant and reliable for use in the event of a disaster. The document owner is responsible for updating the document to ensure that it accurately reflects the customer services provided, contact listing details and additional references that may change from time to time.

Testing Approaches

Testing of the ability to recover business operations at Uplevel will be performed on a scheduled time frame.

The manner in which testing is conducted may include, or exclude a combination of, the following approaches:

- Simulation or scenario testing based on hypothetical disruptions to business operations. This involves stepping through the detailed recovery procedures to ensure they remain relevant to current business operations against hypothetical workshop situations. This includes potentially informing external contacts that a simulation test is being conducted

- Re-service of customer work at an alternate site. This involves confirming the ability to transfer customer requirements, for a hypothetical day to alternate sites, if the loss of Uplevel operations scenario eventuates. The aim of the re-service testing is to obtain comfort that the quality of product required to be generated can be reproduced within the required time frames. Re-service tests are often tested as part of normal operations

- Conduct a Structured Walk-through. A Structured Walk-Through is a paper evaluation of a business continuation plan designed to expose errors or omissions without incurring the level of planning and expenses associated with performing a full operations test. The Structured Walk-Through is, in effect, a role plan of a “disaster” scenario that takes place within the confines and safety of a conference room.

Testing and Maintenance Schedule

Each recovery scenario will be tested annually to confirm the relevance of each detailed recovery process. Other components of the BCP are required to be confirmed as indicated below.

A BCP must have an active maintenance plan to capture the dynamic nature of the business it is built to protect. This ensures that any updates required as a result of testing performed, is promptly updated into the Uplevel BCP.

The below schedule depicts the anticipated time frames in which testing, and subsequently maintenance, will be performed for the BCP components:

Section of BCP	Testing Conducted
Recovery scenario	
Loss of Critical IT Systems / Cloud Provider	Annually
Resource Requirements (e.g. loss of personnel)	Annually

Review/Approve for Content/Compliance

Joe Levy

August 9th, 2020

NAME
Chief Executive Officer

Date

Albert Strong

July 29, 2020

NAME
Chief Information Security Officer

Date

Nimrod Vered

August 17, 2020

NAME
Chief Technology Officer

Date

Version History

Date	Version	Author	Details of Amendment
07222020	1.0	Albert Strong	
08222020	2.0	Albert Strong	
09082020	3.0	Albert Strong	