Uplevel Disaster Recovery Plan

Effective Date: 3/31/2021

Version 7.0 Responsible Party: Albert Strong

Table of Contents

Introduction

Purpose

The purpose of this Information Technology (IT) Disaster Recovery Plan (DRP) is to provide IT staff at UPLEVEL with a documented and detailed plan to ensure the successful recovery of information systems in the event of a catastrophic system outage.

This document contains the information system's DRP to be used along with related documents to respond to an incident that renders the system partially or completely inoperable for over 48 hours, and requires relocation to an alternate processing site. The DRP does not address minor disruptions that do not require relocation.

This DRP describes the overall response plan and details roles and responsibilities. The DRP provides information on the phases of a response, and details the processes involved in those phases.

Scope

This DRP addresses a disaster that mandates the relocation of the system to an alternate the Disaster Recovery Facility. A disaster is defined as a major incident that seriously disrupts, or is expected to disrupt, operations for 48 hours or more, requiring:

- Reassignment of personnel to disaster recovery activities;
- Use of additional vendor/contractor support to accomplish recovery requirements; and/or
- Acquisition of special funding to support equipment replacement and other recovery-related costs that are outside of the scope of normal day-to-day operations.

Operation of systems other than the production UPLEVEL platform is not included in this plan.

Assumptions

This Disaster Recovery Plan is based on the following assumptions:

- The safety of the initial emergency response teams can be assured during the damage-assessment period.
- The contingency period may exist for a period of 180 days or longer if circumstances require.
- Key internal contacts or alternate contacts are available to coordinate the recovery process
- 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.

- Amazon Web Services (AWS) is the designated primary service provider for redundant system capabilities.
- Amazon Web Services (AWS) is the designated alternate service provider for redundant system capabilities.
- If relocation to the alternate service provider is unnecessary because the primary service provider is adequately available for operation and the levels of availability can be maintained with high assurance, then recovery team can commence restoring operations at the primary service provider.
- The designated alternate service provider is not affected by the incident, is operational, and is accessible to UPLEVEL personnel.
- Simultaneous or concurrent incidents at the primary service provider and alternate service provider have not occurred.
- External entities will continue to transmit data to and receive data from UPLEVEL.

- UPLEVEL system backups have been tested and will run on alternate servers.
- Data backup media are undamaged and accessible.
- UPLEVEL teams have the work tools and equipment necessary to complete their tasks.
- UPLEVEL management will support the information resource services recovery and restoration efforts.
- This DRP is not designed for minor, daily operational problems, but for a prolonged service interruption over a defined period of time.
- The DRP is a living document and will be reviewed on a recurring schedule and updated, as necessary. Review period will be annually, or more frequently, as required.

Phases

This Disaster Recovery Plan execution will occur in three phases:

1) Activation

2) Recovery

3) Restoration.

The table below delineates the overarching objectives of each DRP phase.

While the recovery and restoration of UPLEVEL business operations is a priority, the health and safety of UPLEVEL staff is of utmost consideration. All of the following activities are outlined as stated under the assumption that the health and safety of staff can be assured. If the health and safety of staff cannot be assured at the location designated, an alternate location will be provided or the tasking delayed until it was safe to proceed.

Table 1: Disaster Recovery Plan Phase Objectives

Activation
Define the initial actions that should be taken once a disaster has been declared.
Establish an immediate and controlled presence at the incident site(s).
Conduct a preliminary assessment of incident impact, damage, and disruption to the system and components.
Obtain and disseminate information on whether and when availability to the primary facility will be restored.

Activate the Disaster Recovery Plan with consideration for scale of incident.
Provide UPLEVEL management with information to determine requisite recovery.
Recovery
Establish a management control mechanism for the recovery operations.
Activate and mobilize the disaster recovery teams to facilitate and support the recovery process.
Notify and apprise time-sensitive disaster recovery team leads of the situation.
Alert employees, vendors and other internal and external individuals and organizations.
Prepare and implement procedures necessary to facilitate and support the recovery of less time-sensitive functions.
Continue to alert employees, vendors, subcontractors, and other internal and external individuals and organizations on the status of disaster operations.
Reconstitution
Prepare procedures necessary to facilitate the restoration of business operations to the new or repaired facility.
Implement procedures necessary to mobilize operations, support, and technology department restoration.
Manage the migration effort, as well as perform employee, vendor, and customer notification before, during, and after restoration.

Objectives

This Disaster Recovery Plan seeks to document the recovery strategy for UPLEVEL information systems and provide a road map of predetermined actions in order to accomplish the following:

- Minimize the duration of a serious disruption to operations and resources (both information processing and other resources);
- Minimize immediate damage to, and loss of, information assets;
- Establish management succession and escalation procedures;

- Facilitate effective coordination of recovery tasks;
- Identify resources to be used in recovering and reconstituting;
- Reduce the complexity of the recovery effort;
- Develop procedures to be used before, during, and after an event that renders information systems unable to sustain mission-critical functionality;
- Develop appropriate recovery actions for critical production UPLEVEL platform components supporting mission-critical functions;
- Provide for the continuity of UPLEVEL platform services and initial recovery within 48 hours following the declaration of a disaster;
- Maintain recovered operations for at least 180 days.

Personnel

Authority

The Disaster Recovery Plan Coordinator (DRPC) will authorize all changes to the information system Disaster Recovery Plan (DRP). The DRPC will coordinate with each of the disaster recovery teams to ensure the resumption of the system operations during an emergency.

Documented roles and responsibilities ensure that the teams responsible for executing the DRP are aware of the processes and coordination efforts necessary to activate and implement the plan. Most of the team members are technical administrators and specialists from the organization's technology group. There is no minimum or maximum number of team members, but there is sufficient redundancy to cover all requirements in case of team members being unavailable to perform their support.

A single email address in the organization's address book is established so documents or issues can be sent from and to a single address. This provides a permanent e-mail address for security, disaster, and incident response communications that will not have to be changed when organization security personnel are reassigned or leave the organization.

All information pertaining to personnel assigned to Disaster Recovery Teams, including this DRP, is sensitive information. It shall be marked "Sensitive and Confidential" and protected accordingly.

Roles and Responsibilities

Subsequent sections provide a description of each recovery team, the roles and responsibilities for each team, and tables containing general membership for each team. These tables shall be used during an incident to provide status updates to teams and management. Refer to **Appendix E: Disaster Recovery Team and Role Matrix** for a quick-reference chart for each team and an indication of its active status in each disaster recovery phase.

Disaster Recovery Plan Coordinator

The Disaster Recovery Plan Coordinator is the central operations manager and liaison to the executive team. The DRPC monitors the development of the DRP, the conduct of training and awareness, and performance of testing. The DRPC coordinates strategy development with disaster workgroups, team leads, business process owners, and management. Since the maintenance of the plan is an ongoing process, the DRPC routinely updates the plan documentation to ensure all information is kept current. The DRPC and Alternate DRPC are assigned, and their specific responsibilities have been identified and included in their job descriptions.

Table 1: Disaster Recovery Plan Coordinator Assignments

Role	Name
Disaster Recovery Plan Coordinator	Albert Strong
Alternate Disaster Recovery Plan Coordinator	Joe Levy

Line of Succession

This Disaster Recovery Plan sets forth an order of succession to ensure there is someone with decision-making authority for the DRP available at all times. The Line of Succession is located in Appendix L: Senior Management Succession Plan. The Disaster Recovery Plan Coordinator is responsible for activating this plan in the event of a disaster. In the absence of the DRPC, the Alternate DRPC assumes responsibility for all activities assigned to the DRPC.

A Team Lead has been identified for each Recovery Team and is responsible for ensuring the team performs all requisite activities. If a Team Lead is not available, the Alternate Team Lead (second name listed for the team) shall assume the Team Lead responsibilities.

Recovery Teams

Staffing is the key to the success of disaster operations, and teams possess the mix of skills required to resume system operations. The DRPC and various technical and support teams comprise the disaster organization. Most of the team members will be system administrators and technical specialists from UPLEVEL but will be supported by service provider(s), as needed.

Contact information for the team members is located in Appendix D: Disaster Recovery Personnel Contact Information.

Executive Management Team

The Executive Management Team (EMT) is responsible for the executive-level decisions in the period following a disaster and mobilizes the teams to begin recovery activities, including activating the alternate site. The EMT will make policy decisions and serve as the official source of information during the recovery process.

Table 2: Executive Management Team

Title	Name
Chief Executive Officer (CEO)	Joe Levy
Chief Technology Officer (CTO)	Nimrod Vered
Chief Information Security Officer	Albert Strong

Disaster Recovery Plan Management Team

The Disaster Recovery Plan Management Team (DRPMT) is responsible for disaster team coordination, management oversight, progress, and incident tracking. It is tasked with disseminating information within and outside the disaster organization, tracking the status of actions, and tracking and responding to any developments after the initial incidents. It also ensures that future business processes and environmental changes conform to management directives and strategies for this DRP.

Table 3: Disaster Recovery Plan Management Team Assignments

Role / Title	Name
Team Lead	Albert Strong
Alternate Team Lead	Nimrod Vered
Chief Executive Officer (CEO)	Joe Levy

Emergency Response Team

The Emergency Response Team (ERT) is the first responder to an incident. This team assesses the functionality of information system assets, conducts an initial damage assessment, and provides ongoing status to management. Once the ERT has conducted their assessment of the disaster, team members shall disperse to lead other Disaster Recovery Teams.

Table 4: Emergency Response Team Assignments

Role / Title	Name
Team Lead	Nimrod Vered
Alternate Team Lead	Albert Strong

Infrastructure Team

The Infrastructure Team assesses the functional condition of physical facilities, including power, light, heat, ventilation, air conditioning, and water at the affected vendor site. For the purposes of the DRP, the service providers account managers assigned to the Uplevel accounts will coordinate with the identified team members.

Table 5: Infrastructure Team Assignments

Role / Title	Name
Team Lead	Nimrod Vered
Alternate Team Lead	Brian Park
Chief Information Security Officer (CISO)	Albert Strong

Network Installation and Operations Team

In the event of a loss or outage, the Network Installation and Operations Team shall restore data communications links. For the purposes of the DRP, the service providers account managers assigned to the Uplevel accounts will coordinate with the identified team members.

Table 6: Network Installation and Operations Team Assignments

Role / Title	Name
Team Lead	Nimrod Vered
Alternate Team Lead	Brian Park
Chief Information Security Officer (CISO)	Albert Strong

Server Administration Team
The Server Administration Team tests and configures servers that run general system applications. The team's skill sets should be comprehensive enough to address issues involving any system's critical users and critical applications.

Table 7: Server Administration Team Assignments

Role / Title	Name
Team Lead	Nimrod Vered
Alternate Team Lead	Brian Park
Chief Information Security Officer (CISO)	Albert Strong

Platform Application Team
The Platform Application Team retrieves backup copies of applications systems and applications data. Team members are familiar with application operation and data storage to restore Uplevel platform operation.

Table 8: Platform Application Team Assignments Table 7: Network Installation and Operations Team Assignments

Role / Title	Name
Team Lead	Nimrod Vered
Alternate Team Lead	Brian Park
Chief Information Security Officer (CISO)	Albert Strong

Procurement Team
The Procurement Team consists of persons with purchasing authority knowledgeable of the technology resources during normal and emergency operations. Specifically, the team members have knowledge of the budgetary, funding, and acquisition processes required for expedited acquisition of disaster resources. They shall execute emergency acquisitions as required by other teams.

Table 9: Procurement Team Assignments

Role / Title	Name

Team Lead	Joe Levy
Alternate Team Lead	Nimrod Vered

Execution

Activation Phase

Activation Authority

Only designated personnel have the authority to activate the Disaster Recovery Plan. This authority includes the ability to obligate funds to cover expenses from a disaster.

Table 1: Disaster Recovery Plan Activation Authority

Role	Title	Name
Activation Authority	Chief Executive Officer (CEO)	Joe Levy
Alternate Activation Authority	Chief Technology Officer (CTO)	Nimrod Vered

Organization Notification and Activation Procedures

1 All personnel are responsible for notifying Leadership Team of the incident including:

- Time of incident
- Manner in which incident was identified

When: Immediately upon identification of incident

2 The Leadership Team conducts an initial assessment of incident to determine response .

When: 1 – 15 minutes of incident notification

Upon a determination that the incident qualifies as an emergency, the following notification procedures shall be implemented:

1. Activation Authority or Alternate Activation Authority shall notify the Disaster Recovery Plan Coordinator (DRPC) and Alternate DRPC that the DRP is **"Activated."**
2. DRPC shall contact the Team Leads.
3. If a Team Lead is not available the DRPC shall contact the Alternate Team Lead, who shall assume the Team Lead responsibilities.
4. If both the Team Lead and Alternate Team Lead are unavailable, the CTO and DRPC shall designate a person to perform as Team Lead.
5. The Team Lead shall contact the Alternate Team Lead and other team members to provide specific instructions on how to proceed.
6. Initial attempts to contact critical personnel shall not exceed 2 hours. Beyond 2 hours, Team Leads shall designate an individual to continue notification.
7. Team members shall report to a designated meeting place, if necessary. This meeting place is conducted via teleconference.
8. The DRPC shall start a "Disaster Log" to track actions, issues, results, and other information related to the activation and support of the disaster recovery response.

Internal Incident Notification

The DRPC shall notify the Emergency Response Team (ERT). Upon notification, the team shall conduct an initial incident and damage assessment and issue advisory status report(s) to the Disaster Recovery Plan Management Team.

Public Information Release

All incident-related information, printed or spoken, concerning the system shall be coordinated and issued by the Public Information Officer (PIO). The PIO will notify the appropriate internal staff and external organizations as deemed necessary.

Table 2: Public Information Officers

Title	Name
Public Information Officer	Albert Strong
Alternate Public Information Officer	Joe Levy

Activation Phase Teams and Tasks

The tables below identify the tasks and coordination required by the Disaster Recovery Plan Management Team and Emergency Response Team during the Activation Phase. These tables shall be used during an incident response to provide status updates to teams and management.

Table 3: Disaster Recovery Plan Management Team Activation Tasks

Task	Coordination Required
Pre-declaration activities - Communications via direct phone calls and conference calls begin	DPRC
Notify all Disaster Recovery Plan teams to prepare for plan execution.	DRPC
Execute the Organization Communication Plan that informs employees, Vendors and all other interested parties of the disaster and provides updates on the recovery status as information becomes available. Remind Recovery Teams to refrain from discussing the incident with the news media.	DRPC
Assemble the Recovery Teams virtually or at the pre-designated location.	DRPC

Table 4: Emergency Response Team Activation Tasks

Task	Coordination Required
Evaluate the initial status of the damaged infrastructure and any critical services that support its ongoing operation.	ERT
Evaluate the elapsed time before service can be restored.	ERT

Notify DRPC of the status of the extent of the damage and the expected efforts required to restore service.	ERT

Recovery Phase

Recovery Phase Goals and Actions

During the Recovery Phase, the following goals and actions shall apply:

- Establish a management control center for the recovery operations.
- Activate and mobilize the disaster teams to facilitate and support the recovery process.
- Notify and apprise time-sensitive disaster recovery team leads of the situation.
- Alert employees, vendors, and other internal and external individuals and organizations.
- Prepare and implement procedures necessary to facilitate and support the recovery of less time-sensitive functions.
- Coordinate with senior management to discern responsibilities that will fall upon UPLEVEL Inc staff disaster recovery teams.
- Continue to alert employees, vendors, and other internal and external individuals and organizations on the status of disaster recovery operations.
- Maintain the "Disaster Recovery Log."

Recovery Phase Teams and Tasks

The tables below identify the tasks and coordination required by the disaster recovery teams during the Recovery Phase. These tables shall be used during an incident response to provide status updates to teams and management. The following teams are assigned tasks during the Recovery Phase:

- Executive Management Team
- Disaster Recovery Plan Management Team
- Infrastructure Team

Executive Management Team

Table 1: Executive Management Team Recovery Tasks

Task	Coordination Required
Provide the highest level of decision making and oversee the Disaster Recovery effort.	DRPC
Contact Department leaders and discuss the exact nature of the event and the course of action to be followed.	ERT
Oversee the Disaster Recovery effort.	DRPC
Contact recovery site provider to declare a disaster. Disaster declaration reference materials are attached to this plan. This task is the initial responsibility of the Chief Executive Officer. If he/she is unable to perform this task, the task is executed by the Chief Technology Officer. If the CEO or CTO is unable to perform this task, the task is executed by the Chief Customer Officer.	DRPC
Contact Business Partners	PIO
Issue Situation Report	ERT

Disaster Recovery Plan Management Team

Table 2: Disaster Recovery Plan Management Team Recovery Tasks

Task	Coordination Required
Establish operations center	CEO, CTO
Track and receive status updates	Team Leads
Report disaster status to UPLEVEL Inc senior management	DRPC
Disseminate status reports to teams	DRPC
Disseminate decisions and tasking to teams	DRPC
Oversee the activities in the Emergency Response Team, Infrastructure Team, Network Installation & Operation Team, Server Administrator Team, Platform Applications Team, and Procurement Team.	DRPC
Communicate with the DRP Teams to establish priority of restoring the platform functions. This may vary depending on the time of the disaster. When available, notify the Executive Team when the systems are estimated as being operational.	DRPC, Recovery Teams
Conduct and hold periodic meetings, while in disaster mode, in order for the team to regroup.	DRPC, Recovery Teams
Report DRP Teams status updates to the Executive Management. Lead in resolving operational problems and escalate issues to the CTO, if necessary.	DRPC
Perform problem tracking and issue resolution.	DRPC, Recovery Teams
Take the lead to ensure the Disaster Declaration Checklist is completed. Checklist is listed as a document in the Plan.	Team Leads

Infrastructure Team

Table 3: Infrastructure Team Recovery Tasks

Task	Coordination Required
Ensure alternate site is ready for platform relocation	DRPC

Network Installation and Operations Team

Table 4: Network Installation and Operations Team Recovery Tasks

Task	Coordination Required
Ensure alternate site is ready for platform relocation	DRPC
Test remote connections	Multiple Teams

Server Administration Team

Table 5: Server Administration Team Recovery Tasks

Task	Coordination Required
Determine replacement servers	Multiple Teams
Load basic configuration (e.g., operating system, O/S service packs, component software)	Infrastructure Team
Synchronize needed backup files	Platform Application Team
Monitor server performance	Platform Application Team
Implement additional server hardware and software, as needed	Multiple Teams

Optimize server configuration	Platform Application Team

Platform Application Team

Table 6: Platform Application Team Recovery Tasks

Task	Coordination Required
Review backup strategy	Server Administration Team
Obtain needed files for Server Administration Team	Server Administration Team
Monitor restoration	Server Administration Team
Restore non-critical data files	Server Administration Team
Plan for backup of disaster systems	Server Administration Team

Procurement Team

Table 7: Procurement Team Recovery Tasks

Task	Coordination Required
Assemble critical resources (e.g., forms, contracts)	Procurement Team
Process requests for purchases from teams	Multiple Teams

Reconstitution Phase

Reconstitution Phase Goals and Actions

During the Reconstitution Phase, the following goals and actions shall apply:

- Prepare procedures to facilitate the relocation and migration of UPLEVEL Platform operations to the new facility.
- Implement procedures necessary to mobilize operations, support, and technology department relocation or migration.
- Manage the migration effort as well as perform employee, vendor, and customer notification before, during, and after migration.
- Provide documented Lessons Learned drawn from the "Disaster Recovery Log."

Reconstitution Phase Teams and Tasks

The tables below identify the tasks and coordination required by the disaster recovery teams during the Reconstitution Phase. These tables shall be used during an incident response to provide status updates to teams and management. The following teams are assigned tasks during the Reconstitution Phase:

- Disaster Recovery Plan Management Team
- Infrastructure Team
- Network Installation and Operations Team
- Server Administration Team
- Platform Application Team
- Procurement Team

Disaster Recovery Plan Management Team

Table 1: Disaster Recovery Plan Management Team Reconstitution Tasks

Task	Coordination Required
Begin deactivation of Operations Center and Alternate Site	DRPC
Notify UPLEVEL Inc staff of restoration of full service	DRPC
Publish Lessons Learned from disaster recovery operations, as drawn from the Disaster Recovery Log, and review and update Disaster Recovery Plan, as necessary	DRPC

Infrastructure Team

Table 2: Infrastructure Team Reconstitution Tasks

Task	Coordination Required
Identify excess hardware and software	Multiple Teams

Re-allocate excess resources	Multiple Teams
Cancel disaster recovery facilities contract as necessary	Procurement Team

Network Installation and Operations Team

Table 3: Network Installation and Operations Team Reconstitution Tasks

Task	Coordination Required
Ensure new or refurbished permanent facilities are ready for platform migration	DRPC
Test network connectivity in new or refurbished permanent facilities	Service provider(s)

Server Administration Team

Table 4: Server Administration Team Reconstitution Tasks

Task	Coordination Required
Verify system administration setup	Multiple Teams
Restore applications and files	Multiple Teams

Platform Application Team

Table 5: Platform Application Team Team Reconstitution Tasks

Task	Coordination Required
Backup all systems and servers	Multiple Teams
Send backup tapes to offsite storage	DBRT
Restore data on servers at new/reconstituted operations site	Multiple Teams

Procurement Team

Table 6: Procurement Team Reconstitution Tasks

Task	Coordination Required
Close outstanding orders	Multiple Teams
Review contracts for cancellation	Multiple Teams

Appendix A: Primary Service Provider

Service Provider	
Name	AWS
Work Phone	
Physical Address	
Mailing Address	
Point of Contact	
Name	Account Manager
Title	
Work Phone	

Email	

Appendix B: Alternate Service Provider

Service Provider AWS Designated Geographic Back up Data Center	
Name	
Work Phone	
Physical Address	

Mailing Address	
Point of Contact	
Name	
Title	
Work Phone	
Email	

Appendix C: Disaster Recovery Personnel Contact Information

This attachment is a roster of roles prescribed in the Disaster Recovery Plan and key organizational personnel.

Role / Title	Name	Mobile	Email
Disaster Recovery Plan Coordinator (DRPC)/Chief Information Security Officer	Albert Strong	571-214-7446	Albert.strong@strongcybersolutions.com
Team Lead/ Chief Technology Officer (CTO	Nimrod Vered	4254-444-6958	ravs@uplevelteam.com
Chief Executive Officer (CEO)	Joe Levy	206-399-5567	joe@uplevelteam.com
Director of Finance	Brent Abrahamsen	425.941.2429	babrahamsen@countsy.com
Director of Customer Service	Jori Saeger	206-200-5623	jori@uplevelteam.com

Appendix D: Disaster Recovery Team and Role Matrix

A quick-reference chart for each team and an indication of its active status in each disaster recovery phase.

Individual/Team	Major Role	Active in Phase		
		Activation	Recovery	Reconstitution
Chief Technology Officer (CTO)	• Owns the Disaster Recovery Plan. • Makes executive decisions based on the disaster recovery scenario.	✅	✅	✅
Disaster Recovery Plan Coordinator (DRPC)	• Monitors Disaster Recovery Plan development, training and awareness, and testing. • Updates management staff. • Makes operational decisions based on the disaster recovery scenario. • Ensures proper maintenance and testing of the Disaster Recovery Plan.	✅	✅	✅
Executive Management Team	• Oversees the Disaster Recovery Plan to execution.		✅	
Disaster Recovery Plan Management Team	• Ensures business process and environmental changes conform to management directives/strategies for the Disaster Recovery Plan. • Managerial operations team for the Disaster Recovery Plan Coordinator. • Responsible for issuing internal coordination in the Disaster Organization (teams) and external public affairs.	✅	✅	✅

Emergency Response Team	• First responders in the event of an incident. • Conducts initial damage assessment. • Makes initial recommendations to the facilities team. • Informs management.	✅		
Infrastructure Team	• Assesses the functional condition of primary facility. • Takes action in a localized situation or alternate site relocation, as required. • Responds to small-scale fixes once disaster operations are initiated. • Restores data communications links in the event of a loss or outage. • Tests and configures servers that are general file system applications, e.g., user account access to the system, user authentication, general administration and data storage, and e-mail services. • Retrieves backup copies of systems and applications data.		✅	✅
Procurement Team	• Expedites acquisition of needed resources (i.e., information resources and supplies inventory).		✅	✅

Appendix E: Incident Documentation

An Emergency Response Team member shall complete the Initial Incident Response form when a disaster occurs.

Initial Incident Response

ERT Member		Role:		Date:	mm/dd/yy
Brief Synopsis of Incident:					
Assessment:					
Problem/Issue:					
Risk:					
Mitigation Strategy:					
Discussion					
Reviewed By:				Date:	mm/dd/yy
Approved By:				Date:	mm/dd/yy

Appendix F: Action Item Checklist

Task	Completed	Completed By
SYSTEM DISRUPTION—INITIAL NOTIFICATION		
The DRP Coordinator contacts the Recovery Teams and instructs them to perform a damage assessment.		
DAMAGE ASSESSMENT PROCEDURES		
Complete Damage Assessment Report		
Check the cause of the application disruption, including type, scope, location, and time of incident.		
Check whether the outage is localized (this application only) or widespread.		
Check the location of failing components and those users without service.		
Check the impact of the disruption or components damaged.		
Check the functional status of all application components (e.g., fully functional, partially functional, nonfunctional).		
Check the potential for additional disruption or application damage.		
Check the Identification of a single point of failure (if possible).		
Check Items to be replaced (e.g., hardware, software, firmware, supporting materials).		
Check anticipated downtime of the application (e.g., longer than two days).		

Classify disruption as 'Minor System Failure' or 'Major System Failure'.		
MINOR SYSTEM FAILURE		
Recovery and Resumption Procedures		
The Recovery Teams contact the DRPC to provide an estimated recovery time and begin repair of the components (i.e., the databases, servers, infrastructure or the application software).		
The DRPC notifies all users that the 'Minor System Failure' is being recovered and will be functioning under normal conditions within the estimated recovery period.		
Minor System Failure is recovered and incident is closed.		
MAJOR SYSTEM FAILURE		
Notification/Activation Procedures		
The DRPC reviews the damage assessment report and contacts the CEO and CTO to formally activate the disaster recovery plan.		
The DRPC contacts all user groups, altering them of a major system outage and expected recovery time.		
The DRPC contacts all required Recovery Team personnel to initiate system or application recovery.		
Recovery Procedures – Building and Facilities Services		
The DRPC coordinates with Emergency Management Team to obtain an estimated downtime.		
The DRPC provides the Executive Management Team with periodic updates regarding the reopening of the building and the restoration of facilities services.		

Recovery Procedures – IT Infrastructure		
The Network Operations Recovery Team contacts all necessary vendors to provide additional support as needed.		
The Network Operations Recovery Team also obtains and restores data from backup facilities to assist in the restoration of all components.		
The DRPC contacts the Executive Management Team to provide periodic updates on recovery operations as they are received from the Network Operations Recovery Team.		
The DRPC contacts the Executive Management Team upon the recovery of the IT Infrastructure, and disaster operations move into the resumption phase if the application is operating under normal conditions.		
Recovery Procedures – Application Software		
The DRPC notifies the Application Support Recovery Team to begin recovery operations of the application software.		
The Application Support Recovery Team conducts all necessary activities to restore the application software and data.		
The DRPC contacts Executive Management Team to provide periodic updates on recovery operations as they are received from the Application Software Recovery Team.		
The DRPC contacts Executive Management Team upon the recovery of the application software, and disaster operations move into the resumption phase if the application is operating under normal conditions.		
RESUMPTION PROCEDURES		

Recovery Team personnel test all recovered components and application software.		
The DRPC notifies Executive Management Team that the application has been tested and is functioning properly.		
Recovery Teams return all materials, plans, and equipment used during recovery and testing back to storage.		
All sensitive material is destroyed or properly returned to safe storage.		
Recovery Team personnel assisting other offices, conclude their activities and report back to their primary sites.		
The DRPC notifies the user groups regarding the resumption of normal business operations.		
The DRPC develops an after-action report and files it with the Executive Management Team.		

Appendix G: System Backup and Recovery

System Backup Plan

MySQL

MySQL database backups are backed up daily. Backups are retained for up to 14 days' worth of history. Backups are encrypted and are stored in multiple regions to ensure security and availability when needed. Based on the total database size of approximately 1GB the backup restoration process takes five to ten minutes.

Application Artifacts

Application artifacts are archived in an AWS S3 Bucket organized by application version.

System Recovery Plan

MySQL

- Provision Amazon RDS MySQL instance

- use **sg-0f0dfbc2e5329f1cb - rds-launch-wizard-2** as the security group
- Restore MySQL backup to RDS
- Record the
    - Connection URL:
      writer: uplevel-clients-prod.cb3eic793apl.us-west-2.rds.amazonaws.com
      reader: uplevel-clients-prod-us-west-2b.cb3eic793apl.us-west-2.rds.amazonaws.com
    - User Name: level9
    - Password is in 1password

- Change the Dashboard ECS Job task definition to point to the new RDS Instance

Blue DB

- Provision Amazon RDS MySQL instance

- use BlueDB-security (sg-07a567a77aeeed73a) as the security group
- Restore MySQL backup to RDS
- https://us-west-2.console.aws.amazon.com/rds/home?region=us-west-2#snapshots-list:tab=automated
- nightly snapshots
-
- click into the snapshot you want. under 'actions' click restore snapshot.
- menu will ask for vpc/subnetgroup.
-
- you can change the rds size here. the db tech & version need to be the same (should be already set)
-
- Record the
    - Connection URL:
      writer: the-big-blue-reader.cb3eic793apl.us-west-2.rds.amazonaws.com
      reader:
      the-big-blue-db-prod-cluster-instance-1.cb3eic793apl.us-west-2.rds.amazonaws.com

  - User Name: uplevel_rw
  - Password is in 1password

- Change the Dashboard ECS Job task definition to point to the new RDS Instance

Uplevel Dashboard

- Navigate to uplevel-dashboard-ec2-cluster in ECS https://us-west-2.console.aws.amazon.com/ecs/home?region=us-west-2#/clusters/uplevel-dashboard-ec2-cluster/services
- Ensure that EC2 Instances are being automatically provisioned correctly by the ECS cluster (should be automatically spinning up if instances go down)
- If Load Balancer is down, re-provision an EC2 Load Balancer and configure ECS to use new Load Balancer
  - Public DNS Name:client-dash-elb-123619061.us-west-2.elb.amazonaws.com
- Ensure that the task definition is still correctly populated with the correct environment variables (pointing to RDS, etc.)

Blue Service

- Navigate to uplevel-blue-cluster in ECS https://us-west-2.console.aws.amazon.com/ecs/home?region=us-west-2#/clusters/uplevel-blue-cluster/services
- Ensure that EC2 Instances are being automatically provisioned correctly by the ECS cluster (should be automatically spinning up if instances go down)
- If Load Balancer is down, re-provision an EC2 Load Balancer and configure ECS to use new Load Balancer
  - Public DNS Name:uplevel-blue-2045260841.us-west-2.elb.amazonaws.com
- Ensure that the task definition is still correctly populated with the correct environment variables (pointing to RDS, etc.)

Dynamodb

- *Restore UserContentData, UserBookmarks and Tenants table from 'Point in Time Restore'*

Appendix H: Disaster Recovery Plan Testing

Disaster recovery procedures shall be tested periodically to ensure the effectiveness of the plan. The scope, objectives, and measurement criteria of each test shall be determined and coordinated by the

DRPC on a per-event basis. The purpose of testing the Disaster Recovery Plan is to exercise and refine the resumption and recovery procedures, and reduce the potential for failure.

Two kinds of testing shall be used: 1) announced testing and 2) unannounced testing. In an announced test, personnel are instructed when testing will occur, what the objectives of the test are, and what the scenario and parameters will be for the test. Announced testing is helpful for the initial test of procedures. It gives disaster recovery teams the time to prepare for the test and allows them to exercise their skills. Once the team has had an opportunity to run through the procedures and practice and coordinate their skills, unannounced testing may be used to test the completeness of the procedures and to sharpen the team's abilities.

Unannounced testing consists of testing team response and procedures without prior notification. The use of unannounced testing is extremely helpful in preparing a team for a disaster because it focuses on the adequacy of in-place procedures and the readiness of the team. When combined with closely monitored restrictions, unannounced testing helps to create simulated conditions that might exist in a disaster. This kind of testing more closely measures the teams' ability to function under the pressure and limitations of a disaster.

Once it has been determined whether a test will be announced or unannounced, the actual objective(s) of the test must be determined. There are several different types of testing that are useful for measuring different objectives. A recommended schedule for the different types of testing is as follows:

One structured walk-through per year

One integrated business operations/information systems test per year

The DRPC and CTO, along with the Team Leads, shall determine end-user participation in the testing.

Appendix I: Exercise Guidelines and Procedures

Disaster Recovery Plan Walkthrough

The purpose of the Disaster Recovery Plan (DRP) Walkthrough is to validate the contents of the DRP. Objectives of the walkthrough include:

Review content of DRP.

Review the ability to process functions at an alternate site.

Review the ability to effectively retrieve the necessary files, manuals, supplies and equipment.

Review the ability to restore system software at the alternate site.

Ensure personnel have knowledge of the business resumption procedures and manual operations.

Review the ability to meet transportation needs.

Review the ability to notify personnel.

Table Top Exercise

The purpose of the table top is to validate a business area and/or a DRP Team's emergency response, recovery procedures. It also serves to provide a learning opportunity for new team members and others who have not participated in an exercise or actual response to an event within the last couple of years. Objectives of the Table Top exercise include:

Review notification procedures and identify notification requirements.

Gain an enhanced understanding of individual roles and responsibilities when activating the disaster recovery plans.

Evaluate the company's contingency processes and procedures.

Increase knowledge of the company's BRPs and Emergency Response Plan.

Raise emergency management awareness among team members.

Identify areas of improvement.

Prepare team members for participation in a Disaster Drill.

Disaster Recovery Management Drill

The purpose of the Disaster Recovery Management Drill is to validate the process of responding to a local crisis while addressing corporate ramifications. The drill includes the Disaster Recovery

Management Plan Team (DRPMT) and Emergency Response Team (ERT) and builds team and individual crisis management skills. The drill objectives include:

Practice notification, coordination and communications among the company's DRPMT and ERT.

Increase team knowledge and familiarity of the company's DRP and individual team member roles and responsibilities

Validate the effectiveness of plans and procedures for response to service interruption impacting the Platform's daily operations

Practice crisis communication response activities

Demonstrate crisis management, business continuity and recovery operation capabilities

Coordinate appropriate response actions and decisions among the location's DRPMT and with the ERT.

Data Center Drill

The purpose of the data center drill is to test the system recovery efforts for preparedness in the event of a disaster. Data center drills are vital to uncover plan deficiencies and gaps that are documented as test issues. The drill objectives include:

Test the content of DRP.

Test the ability to restore systems software on hardware at the alternate processing site.

Test the ability to effectively retrieve the necessary files, manuals and equipment.

Test the ability to process functions at the alternate processing site.

Data Center Drills test the system recovery efforts for preparedness in the event of a disaster. The drills are vital to uncover plan deficiencies and gaps, which are documented as issues. Regular testing gives technology staff adequate time to resolve recovery issues prior to an actual disaster, helping to ensure a successful recovery. The sections below describe the steps necessary to perform a successful Data Center Drill.

Window and Scope

List all applications which will be tested.

Validate with appropriate business units at Uplevel.

Send confirmation of objectives to the appropriate staff.

Planning

Identify DR Drill participants

Notify participants via email of their participation; request confirmation email to ensure their involvement

Schedule the Data Center Drill

Set and publish date for Kick-off meeting.

Set and publish date for Walk-through meeting.

Set and publish date for Support Team meeting.

Set and publish date for Data Center Drill Follow-up meeting.

Conduct Kick-off meeting.

Conduct Walk-through meeting.

Conduct Support Team meeting.

Test Plans

Receive IT unit test plans.

Receive Business unit test plans.

Review test plans and request corrections as required.

Publish all planning documents weekly to a common area.

Refine and revise plans as required.

Freeze updates to DR plans.

Alternate Site Recovery

Publish communication mechanisms.

Keep the replication link active at all times so production continues to replicate.

Ensure user sign-on have been modified and work for the recovered systems.

Validate the recovered system is working.

Perform test - execute application/business functionality verification and capture evidence of successful recovery.

Capture lessons learned, both positive and negative.

Capture Drill Issues and assign owner for future resolution.

Note and document any drill training gaps concerning roles and responsibilities.

Release the DR Drill applications, infrastructure, and other resources.

Retrospective and Improvements

Populate —Lessons Learned template and Drill Issue Tracking template

Schedule and facilitate meeting with Drill participants to review and evaluate the drill. Discuss both Lessons Learned and Drill Issues

Follow up on open Issues with Issue owners to ensure closure.

Confirm the effectiveness/ineffectiveness of the Drill and provide DRPMT with audit evidence package.

Create formal Executive Summary results letter for distribution.

Update DRPMT/Past Data Center Drills/Previous Data Center Drill objectives spreadsheet.

Update training materials as necessary; schedule special training sessions as required.

Appendix J: Lessons Learned Template

To improve the Disaster Recovery Plan (DRP), evaluate lessons learned during a drill and elaborate via this Lessons Learned Template.

If an issue is identified, ensure it is explained in enough detail to identify root cause and determine remediation. The next drill should accommodate any identified improvements, as required.

Positive lessons learned will be written in enough detail to provide a clear understanding of the immediate and the long-term benefits. It should clearly describe how this was achieved so it will be easily understood and adopted for future use.

Date/Time	Finding	Cause	Actions	Remediation	Owner

Appendix K: Senior Management Succession Plan

If the CEO is unable to carry out her/his duties due to the disaster, then the CTO will resume duties.

If the CTO is unavailable to do so, then the VP of Marketing will resume duties.

Product and Engineering

In terms of the Product and Engineering Organization, if the CTO is unable to carry out her/his duties due to the disaster, the Director of Product will be responsible for the Director of Product Integration's duties.

The Board of directors has the right to revise this succession plan at any time based on business needs and people in role at the time of disaster.

Review/Approve for Content/Compliance

Joe Levy	March 31, 2021
NAME	Date
Chief Executive Officer	
	March 31, 2021
Albert Strong	

NAME	Date
Chief Information Security Officer	
Nimrod Vered	March 31, 2021

NAME Chief Technology Officer	Date

Version History

Review Date	Version	Author	Details of Amendment
7/31/2020	1.0	Joe Levy	
8/12/2020	2.0	Albert Strong	Final Changes
8/31/2020	3.0	Albert Strong	Additional minor changes and signatures
9/09/2020	4.0	Albert Strong	Updates
9/25/2020	5.0	Albert Strong	Updates
10/22/2020	6.0	Albert Strong	Update Appendix G
3/31/2021	7.0	Albert Strong	2021 Edition