Wishes Business Continuity Plan (BCP)

Contents

INTRODUCTION

The purpose of this business continuity plan ("BCP") is to prepare Wishes in the event of extended service outages caused by factors beyond our control (e.g., natural disasters or man-made events), and to restore services to the widest extent possible in a minimum time frame. The plan identifies vulnerabilities and recommends necessary measures to prevent extended service outages. It is a plan that encompasses all Wishes system sites and operations facilities.

The scope of this plan is limited to critical technology and operations elements for Wishes Corporation and its subsidiaries ("Wishes" and/or "Company") and to respond to a Significant Business Disruption ("SBD") by safeguarding employees' lives and Company property, making a financial and operational assessment, quickly recovering and resuming operations, protecting all the Company's books and records, and allowing our customers to transact business. This is a business continuity plan, not a daily problem resolution procedures document.

Our plan anticipates two kinds of SBDs, internal and external. Internal SBDs affect only our Company's ability to communicate and do business, such as a fire in our building(s). External SBDs prevent the operation of the financial markets and usage of our third-party vendors such as a terrorist attack, a city flood, or a wide-scale, regional disruption. Our response to an external SBD relies more heavily on other organizations and systems.

Wishes will maintain copies of its BCP plan and the annual reviews, and the changes that have been made to it for inspection.

Plan Objectives

- Serves as a guide for the Wishes recovery team.
- References and points to the location of any data that resides outside this document.
- Provides procedures and resources needed to assist in recovery.
- Identifies vendors and customers that must be notified in the event of a disaster.
- Assists in avoiding confusion experienced during a crisis by documenting, testing and reviewing recovery procedures.
- Identifies alternate sources for supplies, resources and locations.
- Documents storage, safeguarding and retrieval procedures for vital records.

GOVERNANCE AND OVERSIGHT

Wishes Board of Directors delegates the implementation of this plan to Senior Management and Compliance. This plan is intended to be a living document and as such must be reviewed on a regular basis. The plan will be reviewed semi-annually and exercised on an annual basis. The test may be in the form of a walk-through, mock disaster or component testing. Additionally, with the dynamic environment present within Wishes, it is important to review the listing of personnel and phone numbers contained within the plan regularly. The plan will be stored in a common location where it can be viewed by system site personnel and the Emergency Management Team.

The Board of Directors will be made aware of any deficiencies identified in the review or exercise of this plan.

Responsibilities

Compliance is responsible for ensuring the BCP is updated as changes are made to any covered element of this policy, including changes to physical locations, systems that would be impacted by an outage, vendors or location of physical assets.

The Compliance Department will serve as the Recovery Response Coordinators. Specific responsibilities are as follows:

- Provide electronic copy of plan to all team members via email. Team members must store copy of the plan in a location other than the office workspace.
- Regularly review and update information in the disaster recovery plan (e.g., contact lists, equipment inventories). Communicate with the Emergency Management Team to get up-to-date information periodically.
- Hold initial team meeting to get team members acquainted with the plan and hold annual/semi-annual meetings to review the plan on an ongoing basis
- Maintain an accurate record of the locations of alternate sites, equipment suppliers, data storage locations, and implementation plans.

All employees should keep an updated calling list of their work team members' work, home, cell phone numbers both at home and at work or on a device that would not be impacted by an outage or disaster within Wishes physical location(s). All employees should familiarize themselves with the contents of this plan and have a physical or digital copy available for reference should the plan be invoked.

ASSUMPTIONS

While this plan is meant to provide guidance in the event of a disaster impacting Wishes ability to conduct business and perform the minimal operations to ensure business continues, there are a few key assumptions made that may impact the ability for Wishes and the Response Coordinator to carry out the activities included in this plan. The assumptions are as follows:

- Key people will be available following a disaster.
- This document and all vital records are stored in a secure off-site location and not only survived the disaster but are accessible immediately following the disaster.
- One or more of the alternate locations was unaffected by the disaster and fully functional.
- Computers or other resources are available to operations staff to continue conducting business.
- Critical vendors and/or alternative vendors are available and operational in a normal or near-normal capacity.

DISASTER DEFINITION

Any loss of utility service (power, water), connectivity (system sites), or catastrophic event (weather, natural disaster, vandalism) that causes an interruption in the service provided by Wishes operations. The plan identifies vulnerabilities and recommends measures to prevent extended service outages.

A national disaster such as war is beyond the scope of this plan.

INSTRUCTIONS FOR USING THE PLAN

Invoking the plan

This plan becomes effective when a disaster occurs. Normal problem management procedures will initiate the plan and remain in effect until operations are resumed at the original location, or a replacement location and control is returned to the appropriate functional management.

Disaster declaration

The Emergency Management Team and Emergency Response Coordinator are responsible for declaring a disaster and activating the various recovery teams as outlined in this plan.

Notification

Regardless of the disaster circumstances, or the identity of the person(s) first made aware of the disaster, the Emergency Management Team (EMT) must be activated immediately in the following cases:

- Operations system and/or primary operating facility is down **for five (5)** or more hours
- Any problem at any system or network facility that would cause the above condition to be present or there is certain indication that the conditions are about to occur (as is the case with certain natural disasters that can be forecast or tracked, such as a hurricane).

External communications

The Chief Executive Officer ("CEO") is designated as the principal contact with the media (radio, television, and print), regulatory agency, government agencies and other external organizations following a formal disaster declaration. Posts on social media, such as Twitter, Facebook or LinkedIn must be reviewed by the Emergency Management Team and the Compliance Officer prior to distribution. Additional communications via any medium must be approved unless or until instruction is given to allow such information to be released. Any information posted about an outage or other disaster recovery efforts should conform to the Social Media Guidance included in the Customer Contact Policy.

Data Backup Plan

Full and incremental backups preserve corporate information assets and should be performed on a regular basis for audit logs and files that are irreplaceable, have a high replacement cost, or are considered critical. Backup media should be stored in a secure, geographically separate location from the original and isolated from environmental hazards. This will be managed through Hetzner.

All digital data is backed up nightly and stored to Hetzner.

Off-site Storage Procedures

Physical files will be stored with a digital backup. In the instance of a physical file being required, it will be

stored both on-site and duplicated with our secure custodian.

EMERGENCY MANAGEMENT PROCEDURES

The following procedures are to be followed by system operations personnel and other designated Wishes personnel in the event of an emergency. Where uncertainty exists, the more reactive action should be followed to provide maximum protection and personnel safety.

In the event of any situation where access to a building housing a system is denied, personnel should contact their supervisor to determine if they should report to alternative locations.

Natural Disaster

In the event of a major catastrophe affecting a Wishes facility, immediately notify the CEO, who will initiate BCP procedures.

STEP	ACTION
1	Notify Emergency Response Coordinator (CTO) of a pending event, if time permits.
2	If impending natural disaster can be tracked, begin preparation of site within 72 hours as follows: ● Notify senior management ● Prepare for replacement workspace(s) ● Inform other offices of impending natural disaster and need to transfer additional duties ● Prepare phone system ● Develop recommendation for employees and deploy recommendation ● Prepare physical documents to be shipped to custodians ● Review and deposit all outstanding physical checks ● Find replacement location for physical checks for Treasury ● Ensure all Treasury personnel have access to workspace or replacement workspace ● Verify phone numbers on the Call Trees
3	24 hours prior to event (if known): ● Create an image of the system and files ● Backup critical system elements ● Communicate BCP and alternative workspace with all employees

Fire

In the event of a fire or smoke in any of the facilities, the guidelines and procedures in this section are to be followed.

If fire or smoke is present in the facility, evaluate the situation and determine the severity, categorize the fire as *Major* or *Minor* and take the appropriate action as defined in this section. Call 911 as soon as

possible if the situation warrants it.

Wishes employees are to attempt to extinguish minor fires (e.g., single hardware component or paper fires) using hand-held fire extinguishers located throughout the facility. Any other fire or smoke situation will be handled by qualified building personnel until the local fire department arrives.
In the event of a major fire, call 911 and immediately evacuate the area.
In the event of any emergency, system site security and personal safety are the major concern. If possible, the operations supervisor should remain present at the facility until the fire department has arrived.

In the event of a major catastrophe affecting the facility, immediately notify the Emergency Response Coordinator as soon as the fire department is called, and employees are evacuated.

STEP	ACTION
1	Dial 9-1-1 to contact the fire department
2	Immediately notify all other personnel in the facility of the situation and evacuate the area.
3	Alert emergency personnel on: Provide them with your name, extension where you can be reached, building and room number, and the nature of the emergency. Follow all instructions given.
4	Alert the Emergency Response Coordinator. He/she will notify the Emergency Management Team Coordinator.
5	Notify Building Security, if on-site security staff Local security personnel will establish security at the location and not allow access to the site unless notified by the Emergency Response Coordinator or his designated representative
6	Contact appropriate vendor personnel to aid in the decision regarding the protection of equipment if time and circumstance permit
7	All personnel evacuating the facilities will meet at their assigned outside location (assembly point) and follow instructions given by the designated authority.

Network Service Provider Outage

In the event of a network service provider outage to any facility, the guidelines and procedures in this section are to be followed.

STEP	ACTION
1	Notify Emergency Response Coordinator of outage. Determine cause of outage and timeframe for its recovery.
2	If outage will be greater than 2 hours, alternative plans and/or replacement workplace will be communicated to employees. If it is a major outage and all carriers are down and downtime will be greater than 12 hours, employees will be notified of alternative plans and/or locations.

Flood or Water Damage

In the event of a flood or broken water pipe (not due to natural disaster) within any computing facilities or business operations areas with electronic equipment, the guidelines and procedures in this section are to be followed.

STEP	ACTION
1	Assess the situation and determine if outside assistance is needed.
2	Immediately notify all other personnel in the facility of the situation and to be prepared to cease operations accordingly.
3	If water is originating from above the equipment, power down the individual devices and cover with protective shrouds, if possible.
4	Water detected below the raised floor may have different causes: —If water is slowly dripping from an air conditioning unit or other visible source and not endangering equipment, contact repair personnel immediately. —If water is of a major quantity and flooding of the facility is occurring, immediately implement power-down procedures. While power-down procedures are in progress, evacuate the area and follow supervisor's instructions.

Pandemic or Health-Related Event

In the event of a pandemic or local health-related event, the procedures in this section are to be followed.

Prior to a pandemic or health-related issue, the Emergency Response Coordinator, in coordination with Senior Management, will identify roles that are essential to Wishes and must be conducted on-site, if any.

At the outset of a pandemic, as determined by Federal or state government or health agencies, such as the World Health Organization or the Center for Disease Control, the Emergency Response Coordinator is responsible for monitoring the situation and providing information back to the Emergency Response Team, including direction from local, state or Federal agencies.

Wishes will follow any local, state or federal mandates regarding social distancing and may allow for additional roles to work from home to help enable lower staff numbers in the office. Wishes will follow any government orders to shelter in place by allowing staff to take personal work equipment such as monitors and keyboards, as well as office supplies to ensure they are able to carry out their assigned duties. Company meetings will continue remotely if employees have access to connectivity and equipment. Wishes will provide information to employees on how to obtain or order approved resources. Wishes management will continue to communicate with employees to inform of any company updates.

Wishes maintains procedures as business-as-usual to take safety precautions in making necessary cleaning supplies and sanitizers available to staff.

While monitoring any potential health-related issue, it is essential to ensure risk mitigation factors are implemented to reduce the likelihood of transmission throughout the organization or others in a shared workspace facility. Social distancing, increased hygiene and vaccination information will be provided, if available.

During a health-related issue, the Emergency Management Team will coordinate with IT to ensure all employees can connect to Wishes network remotely and will take steps to provide necessary equipment or access.

Wishes will continue to monitor guidelines and mandated orders. Once orders are lifted, management will assess the level of risk prior to returning staff to physical office locations. Once Wishes management determines it is safe to return to the office, details will be provided to impacted employees to coordinate their return to the office.

RECOVERY TIME OBJECTIVE TIMELINE

The Business Continuity Plan Recovery Time Objective (RTO) timeline is broken in to the following two phases:

- Alert/Action Phase
- Monitoring and Recovery Phase

Alert Phase

The Alert Phase of the timeline is the time starting at identification of the issue through the first 2 hours of business interruption.

In addition to following the step-by-step procedures as identified in the above sections, the Emergency Response Coordinator is responsible for gathering relevant information, communicating with the Emergency Response Team and taking appropriate action to assess the extent of the damage and begin steps to recovery.

1. **Notification of incident affecting the site**
   - **If during work hours:**
     Upon observation or notification of a potentially serious situation during working hours at a system/facility, ensure that personnel on site have enacted standard emergency and evacuation procedures if appropriate and notify the Emergency Response Coordinator.
   - **If outside of work hours:**
     Immediately contact the Emergency Response Coordinator (Chief Technology Officer (“CTO”)).

2. Provide status to the Emergency Management Team

The Emergency Response Coordinator will contact the Emergency Management Team (EMT) and provide the following information when any of the following conditions exist:

- Operations system and/or primary operating facility is down for five (5) or more hours; or

- Any problem at any system or network facility that would cause either of the above conditions to be present or there is certain indication that either of the conditions are about to occur.
    - Wishes will continuously to backup to the cloud.

The EMT will provide the following information:

- Location of disaster
- Type of disaster (e.g., fire, hurricane, flood)
- Summarize the damage (e.g., minimal, heavy, destruction)
- Emergency Command Center location and phone contact number; a meeting location that is close to the situation, but away from the disaster scene
- An estimated timeframe of when a damage assessment group can enter the facility (if possible)

3. **Decide course of action**

Based on the information obtained, the EMT decides how to respond to the event.

4. Communicate action to employees

If a disaster is not declared, the Compliance team will continue to address and manage the situation through resolution and provide status updates to Emergency Management.

If a disaster is declared, the Emergency Response Coordinator will notify the Emergency Management Team members immediately for deployment.

A disaster should be declared if a situation is not likely to be resolved within the predefined timelines. The person authorized to declare a disaster must also have at least one backup who is also authorized to declare a disaster in the event the primary person is unavailable.

Using the company call list, the Emergency Management will contact employees to inform them of the situation. If known, advise as to when operations will be restored or what actions will be taken to restore operations.

5. **Emergency Management Team reports to Command Center**

Under the direction of local authorities and/or the Emergency Management Team, Wishes will assess the damage to the affected location(s) and/or assets. The assessment should Include vendors/providers of installed equipment to ensure that their expert opinion regarding the condition of the equipment is determined as quickly as possible.

The assessment should be done using the forms included in the appendices of this program document.

Building access permitting, the Emergency Response Coordinator and/or the Emergency Management team should:

- Conduct an on-site inspection of affected areas to assess damage to essential hardcopy records and electronic data.
- Obtain information regarding damage to the facility.
- Develop a restoration priority list, identifying facilities, vital records and equipment needed for resumption of activities that could be operationally restored and retrieved quickly.
- Develop a Salvage Priority List identifying sites and assets that could be salvaged.
- Make recommendations for required resources.

6. Decide whether to continue to business recovery phase

The EMT decides whether to continue to the business recovery phase of this plan. If the situation does not warrant this action, continue to address the situation at the affected site (s).

The business recovery phase of this plan will be implemented when resources are required to support full restoration of system and/or facility functionality at an alternate recovery site (e.g., another company office, vendor hot site, cold site) that would be used for an extended period.

> **Note: During the Initial Response Phase, service may be shifted to alternate sites to allow operations to begin functioning and provide service to its customers. Initially reduced service may be provided until sites can be fully restored. Within 72 hours/3 days, the system and facilities should be functional at 100%.**

Business Recovery Phase

This section documents the steps necessary to activate business recovery plans to support full restoration of systems or facility functionality at an alternate/recovery site that would be used for an extended period. Coordinate resources to reconstruct business operations at the temporary/permanent system location, and to deactivate recovery teams upon return to normal business operations.

1. Notify technical support staff/coordinate relocation to new facility/location

See Appendix A for Technical Support staff contacts associated with a new location being set up as a permanent replacement location.

2. Secure funding for relocation

The Emergency Management Team will decide in advance with suitable backup location resources. Decide in advance with local banks, credit card companies, hotels, office suppliers, food suppliers and others for emergency support at the new facility, depending on the severity and potential duration of the use of the alternative site.

3. Operations recovered

Assuming all relevant operations have been recovered to an alternate site, and employees are in place to support operations, the company can declare that it is functioning in a normal manner at the recovery location.

4. Recovery Point Objective (RPO).

This parameter is measured in time: from the moment a failure occurs to our last valid data backup. Since our app and app data is managed in the cloud, our RPO will be <5 hours. For all other business operations data including, management, team, website it will be <24 hours.

VERSION CONTROL

Version	Date	Owner	Reviewed By	Approved By	Updates
1.1	November 2022	Wishes	Chase Harmer	Alex Galert	N/A
1.2	July 2023	Wishes	Annie Rhodes	Alex Galert	Team
2.0	August 2023	Wishes	Annie Rhodes		

Appendix A: Wishes Emergency Management Team

Charter

Responsible for overall coordination of the disaster recovery effort, evaluation and determining disaster declaration, and communications with senior management

Support activities

Emergency Management Team:

- Evaluate which recovery actions should be invoked
- Evaluate and assess damage assessment findings
- Set restoration priority based on the damage assessment reports
- Acts as a communication channel to teams and major customers
- Work with vendors to develop a rebuild/repair schedule
- Gather damage assessment information
- Establish command center and related operations.
- If no disaster is declared, then take appropriate action to return to normal operation using regular staff.
- Prepare post-disaster debriefing report
- Coordinate the development of site-specific recovery plans and ensure they are updated semi-annually.
- Coordinate resumption of voice and data communications
    - Coordinate resumption of information system operations:
    - Provide recovery support to the affected location and operations

Emergency Management Team (EMT)

Name	Position/Title	Email Address	Address	Mobile/Cell Phone
Alex Galert	CTO	Alex@wishes.inc	Carl-von-Linné-Str. 1 50226 Frechen Germany	+49 171 1254075
Mitch Trulli	CPO	Mitch@wishes.inc	92 Hicks Ave Medford, MA 02155	+ 978 404 6916
Annie Rhodes	CEO	Annie@wishes.inc	42 Hazelton Dr White Plains, NY 10605	+ 914 629 3393
Chase Harmer	Founder	Chase@wishes.inc	2020 Red Drive Reno, NV 89502	+ 408 857 7759

Appendix B: Emergency Numbers by Location

First Responders, Public Utility Companies, Others

Utility Name	Contact Name	Phone
PG&E		1 (800) 743-5000
Verizon Wireless		+1 800-922-0204
Police Department		911
Fire Department		911
Hospital:		911
Hospital: (Emergency)		911
Internet Support	Comcast	266278 (COMCST) - Txt
Network Support	Comcast Spectrum	855.860.9068

Appendix C: Emergency Command Center (ECC)

Remote Team

Appendix D: Minimum Acceptable Recovery Configuration

The minimum acceptable recovery configuration includes the following:

- 1x laptop per employee
- 1x desk and chair per employee
- 1x office access keycard per employee
- 1x large television monitors or projectors
- Wireless internet of sufficient speed
- Keycard or physical key locking door entry
- 1x fireproof safe
- Basic office facilities

Appendix E: Forms

Incident/Disaster Form

Upon notification of an incident or disaster situation the On-Duty Personnel will make the initial entries into this form. It will then be forwarded to the ECC, where it will be continually updated. This document will be the running log until the incident/disaster has ended and "normal business" has resumed.

TIME AND DATE

_____

TYPE OF EVENT

_____

_____

_____

_____

_____

_____

LOCATION

_____

_____

BUILDING ACCESS ISSUES

_____

_____

PROJECTED IMPACT TO OPERATIONS

_____

_____

RUNNING LOG (ongoing events)

Critical Equipment Status Form

CRITICAL EQUIPMENT STATUS
ASSESSMENT AND EVALUATION FORM

Recovery Team: _____

	[----------STATUS----------]		
Equipment	Condition	Salvage	Comments
1. _____	_____	_____	_____
2. _____	_____	_____	_____
3. _____	_____	_____	_____
4. _____	_____	_____	_____
5. _____	_____	_____	_____
6. _____	_____	_____	_____
7. _____	_____	_____	_____
8. _____	_____	_____	_____
9. _____	_____	_____	_____
10. _____	_____	_____	_____
11. _____	_____	_____	_____
12. _____	_____	_____	_____
13. _____	_____	_____	_____
14. _____	_____	_____	_____
15. _____	_____	_____	_____

LEGEND

Condition:
OK - Undamaged
DBU - Damaged, but usable
DS - Damaged, requires salvage before use
D - Destroyed, requires reconstruction

Appendix F: Building Evacuation Information

Remote, no evacuation procedures

Appendix G: Loss of Technology

Wishes operates with a decentralized executive team which manages the core business using network technology. Because of this setup, Wishes aims to keep the business operational with at least one executive available and therefore any significant natural disaster in one area will not impact the continuity of the company. This plan therefore concentrates on the loss of networking technology because it is the most likely event to occur. For any civic or natural disasters, team members should always follow the direction of response personnel in their area and report their status to the team as soon as practicable.

The priority of the technology systems and the Company's tolerance for unavailability of each system is noted below.

System	Tolerable Outage	Tolerable Data Loss
Cloud Service Provider	30 minutes	60 Minutes
Database Services	30 minutes	60 Minutes
Network and Remote Access	One day	All (no persistence needed)
Email	Three days	Two weeks
File Servers	One day	One month
Phones (Mobile)	Three days	All (no persistence needed)
Payroll	One week	One week
Client Management System	One month	One month
Accounting System	One week	One week
Website	One week	One week

Business Continuity Plan

1. Cloud Service Provider

The primary cloud provider for Wishes is Amazon Cloud Services. The primary interruption risk associated with Amazon Cloud Services is the Company's inability to access the system as a whole. Redundancy is maintained throughout the cloud by deploying multiple instances of the Wishes system across two or more geographic regions. This allows the Company to continue operations without a problem even if an entire geographic region goes offline. The two main regions used within Amazon Cloud Services are US East and US West. The following procedure outlines the recovery process in the event of a total loss of Amazon Cloud Services

Characteristic of Interruption: Loss of Amazon Cloud Services

Short Term (Up to 30 minutes)

Amazon Cloud Services is a primary provider of cloud infrastructure on which many internet-based companies are run. A loss of the entire system would impact a large majority of the internet community and Google Cloud customers can expect regular updates from numerous sources including Amazon Cloud Services itself and the national news. Wishes would stay apprised of all updates and begin to look at implementing the long-term continuity plan when appropriate.

Long Term (More than 30 minutes)

Wishes maintains systems as code, also known as "Infrastructure as Code". This enables the Company to deploy required resources using an infrastructure specific codebase that automatically provisions needed resources with any cloud provider including [Google Cloud] and [Microsoft Azure]. Additionally, Wishes maintains its primary codebase in portable images which can be deployed on any operating-based system (Android, Linux, Apple). Wishes would engage with a new cloud provider to provision needed resources and re-deploy the codebase on these resources to become operational.

2. Database Services

Wishes uses Google Cloud SQL for database services. Additionally, all digital data is backed up nightly and stored to Hetzner. Please refer to the Data Backup Plan section above for more details.

3. Network & Remote Access

Wishes uses the internet as its primary means of communication and coordination. All team members work remotely due to the Cloud setup of the Company, they are able to work remotely, which reduces the company's reliance on any one single service provider and allows for redundancy over a wide geographic area - even for its core team. The primary risk associated with this setup is an extended loss of internet connectivity for any one team member.

Characteristic of Interruption: Loss of Internet for a Team Member

Short Term (Up to 1 day)

The affected team member should notify the [Chief Technology Officer or Designated Responsible Individual] and continue with assigned tasks for the day.

Long Term (More than 1 day)

The affected team member should use alternative communication methods, such as mobile phone, and keep the [Chief Technology Officer or Designated Responsible Individual] up to date regarding their situation. If the internet is expected to remain out of service, then the Company will begin looking at alternative work locations with the member.

4. Email

Wishes currently relies on Gmail to provide web-based email services. In order to use this service, each team member maintains their own internet connection and an email disruption would include either Gmail becoming unavailable or any particular individual losing their internet service.

Characteristic of Interruption: Email Servers Down

Short Term (Up to 3 days)

The [Chief Technology Officer or Designated Responsible Individual] will stay abreast of any updates from Gmail. Affected users will use alternative communication methods such as Wishes' internet messaging service and mobile phone.

Long Term (More than 3 days)

The [Chief Technology Officer or Designated Responsible Individual] will set up a new email service provider and migrate email addresses and files to the new provider.

Characteristic of Interruption: Loss of Internet Service for a Team Member

Short Term (Up to 3 days)

The affected team member should use alternative communication methods, such as mobile phones, and provide daily updates to the [Chief Technology Officer or Designated Responsible Individual].

Long Term (More than 3 days)

The affected team member should advise the [Chief Technology Officer or Designated Responsible Individual] and begin setting up a new internet service provider. If the internet is expected to remain out of service for the affected team member, then the Company will begin looking at alternative work locations with the member.

5. File Servers

Files relevant to Wishes' business operations are maintained with Hetzner, a separate remote location and no physical on-site server system is used. By maintaining redundancy with the file store, backups of important files are always available and accessible. The location for keeping file storage for Wishes is Google Workspace.

6. Phones – Mobile Phone

Each team member is responsible for maintaining their own mobile phone service. If any team member does not intend on maintaining mobile phone services for themselves, they should notify the [Chief Technology Officer or Designated Responsible Individual] in advance. The following applies if any team member's mobile

service is unexpectedly interrupted.

Characteristic of Interruption: Mobile Phone Service Not Working

Short Term (Up to 3 days)

The affected team member should notify the [Chief Technology Officer or Designated Responsible Individual] via email or internet messaging.

Long Term (More than 3 days)

The affected team member should use alternative communication methods and keep the [Chief Technology Officer or Designated Responsible Individual] up to date regarding their situation. If the mobile service is expected to remain out, then the Company will begin looking at alternatives with the team member.

7. Payroll

Wishes uses Intuit to manage payroll services. Intuit maintains disaster recovery processes in accordance with the payroll industry's standards. Wishes mitigates the risk based on Intuit becoming unavailable.

Characteristic of Interruption: Intuit Servers Down

Short Term (Up to 1 Week)

The [Chief Technology Officer or Designated Responsible Individual] will advise Intuit customer support of Wishes' inability to connect with their system and stay up to date on any changes.

Long Term (More than 1 Week)

The [Chief Technology Officer or Designated Responsible Individual] will use back up data to establish a new payroll service provider.

8. Client Management System ("CMS")

Wishes uses Google Workspace as the primary client management system. Risk associated with the client management system is the Google Workspace system becoming unavailable.

Characteristic of Interruption: Google Workspace Servers Down

Short Term (Up to 1 month)

The [Chief Technology Officer or Designated Responsible Individual] will establish a backup spreadsheet in Wishes shared file system as the primary CMS tool and communicate the update with the team members and relevant stakeholders.

Long Term (More than 1 month)

The [Chief Technology Officer or Designated Responsible Individual] will establish a relationship with a new CMS service provider and migrate back up data.

9. Accounting System

Wishes uses QuickBooks as a primary accounting tool provider. The primary risk Wishes aims to mitigate is the loss of access to the accounting system.

Characteristic of Interruption: QuickBooks Servers Down

Short Term (Up to 1 week)

Wishes' primary financial records are maintained in partnership with an accounting firm, currently Stephens, Reidinger & Beller LLP. A loss of access to QuickBooks only results in a loss of convenience tools to generate reports and reconcile expenses. Back up accounting data will be maintained in the file system.

Long Term (More than 1 week)

The [Chief Technology Officer or Designated Responsible Individual] will establish a relationship with a new accounting service provider and migrate back up data.

10.Website

Wishes uses GoDaddy to host the website https://www.wishes.inc/. The same redundancy found in the section Cloud Service Provider is applied to the website and the same procedures will be followed in the event of a complete loss of the cloud provider's system.

Contact List

Team Member Call Tree

Name	Title	Phone	Email
Annie Rhodes	Chief Executive Officer ("CEO")	914-629-3393	Amerhodes@gmail.com
Alex Galert	Chief Technology Officer ("CTO")	+49 171 1254074	itmann@gmail.com
Chase Harmer	Chief Strategy Officer ("CSO")	408-857-7759	Chase.harmer@icloud.com
Mitch Trulli	Chief Product Officer ("CPO")	+ 978 404 6916	mitchelltrulli@gmail.com