FIRM NAME

RECOVERY/BUSINESS CONTINUITY PLAN

PREPARED BY rEDHAWK wEALTH aDVISORS

fOR ALL ADVISORS IN-NETWORK.

Nov 30th, 2021

| VERSION HISTORY | | | | |
| --- | --- | --- | --- | --- |
| VERSION | APPROVED BY | REVISION DATE | DESCRIPTION OF CHANGE | AUTHOR |
| 1.0 |  |  | Policy Creation | Kenny Wong |
| 1.1 |  | 11-29-21 | Policy Review | Taylor Bullard |
| 1.x | IT manager name | Date | Customize to company | Your name |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **PREPARED BY** | Kenny Wong | **TITLE** | IT Manager (former) | **DATE** | MAY 2021 |
| **MODIFIED BY** | Taylor Bullard | **TITLE** | IT Manager (current) | **DATE** | NOV 2021 |

# TABLE OF CONTENTS

[TABLE OF CONTENTS 2](#_Toc72488496)

[1. High-Level Outline of Disaster Recovery Plan 3](#_Toc72488497)

[2. Key Personnel and Contact Information 3](#_Toc72488498)

[3. Information Services Backup Procedures 3](#_Toc72488499)

[4. Disaster Recovery Procedures 4](#_Toc72488500)

[5. Recovery Plan for Mobile Site 5](#_Toc72488501)

[6. Restoration Process 5](#_Toc72488502)

[7. Recovery Plan Practice and Exercising 6](#_Toc72488503)

[8. Disaster Site Rebuilding 6](#_Toc72488504)

[9. Plan Changes or Updates 7](#_Toc72488505)

# High-Level Outline of Disaster Recovery Plan

These are the major goals of the disaster recovery plan.

|  |
| --- |
| * To minimize interruptions to normal business operations * To limit the extent of disruption and damage * To establish alternative means of operation in advance * To train personnel with emergency procedures * To have an established policy in place for smooth and rapid restoration of services |

# Key Personnel and Contact Information

These are the key resources involved in the disaster recovery plan, including all key stakeholders and third-party resources.

Please enter the appropriate info into the blank fields for your office/organization.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **NAME & TITLE** | **ROLE** | **PHONE** | **ALT PHONE** | **EMAIL** |
| Name & Title | Role | Phone # | Alt Phone | Email address |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Information Services

These are the covered systems that would be impacted in case of disaster or major disruption in processes.

|  |
| --- |
| **Instructions**: *Customize this section with systems that are essential to day-to-day business activities. Below is a start to what info should be entered but it must be customized to your company.*  All information is stored on the cloud through various Software as a Service applications. Below is a list of the applications used and a brief description of the service.  Microsoft Office Suite: Software used for business purposes  + Teams: This is our communications hub, linking chat, video conferencing, file shares, advisor data together for our use.  + Outlook: Our primary email comms system.  +Microsoft OneDrive: All documents are backed up using Microsoft OneDrive. Users are able to access files as needed. OneDrive serves as a ‘wrapper’ containing our file share system within an MS SharePoint Online site of the same name.  Orion: Billing and portfolio management software  Redtail: Client relationship management software |

# Disaster Recovery Procedures

These are the key components in the DRP that should be immediately addressed and acted upon in the event of emergency.

|  |
| --- |
| Emergency Response: The following steps are taken when an emergency is/has taken place. An emergency is considered any circumstance that disrupts operations, causes physical or environmental damage to the main office location, and/or major unforeseen disasters that seriously impairs or halts normal business operations. All plans below should be documented with as much information as possible with accompanying timestamps.  Evacuation plan:   1. Employees will be notified to evacuate the building. 2. Employees should meet at the designated assembly area: **Instructions**: *Insert location*. 3. The key team member **Instructions**: *Insert key team member’s name* will confirm that all employees and visitors are at the designated assembly area. 4. The key team member will communicate with the building manager(s) as needed. 5. When given the “all clear” from authorities, employees and visitors are allowed to return to the building.   Severe weather/Tornado sheltering plan:   1. The key team member will monitor weather sources for updated emergency instructions and direct employees and visitors to the designated tornado shelter **Instructions**: *Insert location*. 2. Once the “all clear” is given, employees and visitors may return to normal business functions.   Medical emergency plan:   1. If a medical emergency is report, dial 9-1-1 and request an ambulance if needed. 2. Any trained employee should administer first aid. The first aid kit can be found **Instructions**: *Insert location*. 3. For any complications that are outside of the first aider’s comfortability level, only trained responders should provide first aid assistance. 4. Do not move the victim unless the victim’s location is unsafe. 5. Control access to the scene. 6. Take universal precautions to prevent contact with body fluids and exposure to bloodborne pathogens. 7. Meet the ambulance at the nearest entrance or emergency access point; direct them to victim(s).   Fire emergency plan:   1. If a fire is reported, pull the fire alarm to warn occupants to evacuate. 2. The key team member is to account for all employees and visitors at the designated assembly area. 3. Meet with the building fire emergency contact to inform them everyone is accounted for. 4. Provide updates to the team as they come up.   Pandemic Response: In the event of a pandemic, the following precautions will be taken. A pandemic is considered an event where an infectious disease has spread over a large region and affects a substantial amount of the population. Normal business functions will continue but with additional precautions to ensure the safety of employees.   1. To help stop the spread of disease, disinfect surfaces that are frequently touched, cover coughs and sneezes with a tissue, stay at home if you are sick, and wash your hands often with soap. 2. Employees are allowed to work from home as needed. 3. Increase space between workstations. 4. Postpone or cancel any non-essential work-related travel. 5. Stay up to date on latest developments about the pandemic. 6. Provide any preventative supplies for the workplace as needed. 7. The pandemic response precautions will be updated as needed with company policy changes or government/health department recommendations.   Security Breach (Potential and Confirmed): In the event of the loss of any devices used for work purposes (computer, mobile device, etc.) or the loss of access to covered SaaS systems (M365, Redtail, Orion etc.), the following procedures will be executed without delay.   1. The company will notify the IT Security Contact immediately, either via email or phone. 2. The company will collect all relevant information including which system was affected, exact time it happened, exact location it happened, how the breach was found, and if the affected resource can still be accessed. All details will be shared in the email or phone call with the IT Security Contact. 3. Triage: The IT Security Contact will attempt to separate the resource from other company resources to protect the rest of the system. All passwords related to the breach will be changed immediately, IP and/or geo-locks will be enabled (if applicable), and all systems will be checked immediately to ensure that multi-factor authentication is enabled. 4. The company will make a good-faith investigation into whether end-customer data was corrupted or stolen. All applicable state and federal laws regarding customer notification will be followed in their entirety. This communication will be handled by the IT Security Contact and/or legal representatives as needed. 5. Systems that are recovered (both physical assets and accounts) will be audited to determine if any future security issues are still present. Recovered laptops or mobile devices will go through a factory reset before they are allowed to connect to company resources again. 6. For all security events, an “After Action” report will be created by the IT Security Contact to determine if any procedures were mishandled and how a similar situation will be mitigated in the future. |

# 

# Recovery Plan for Mobile Site

This is the relevant information needed to continue recovery plans at a mobile site.

|  |
| --- |
| If a disaster were to occur, the below steps should be taken.   1. Determine the scope of the disaster. 2. If employees are not able to work from the office for normal business operations, employees should work **Instructions**: *Enter location whether from home or a designated remote work site*. 3. **Instructions:** *Remove if not true for your company and enter location of the designated remote work site*. Most systems are hosted on the cloud and are able to be accessed anywhere. A designated remote ‘work’ site is not required to maintain continuity if internet fails in the home office. 4. If phones need to be forwarded, they will be forwarded to a reachable number. 5. **Instructions:** *Remove if not true for your company and enter location of the designated remote work site*. Employees are to continue normal business operations from home. |

# Restoration Process

These are the steps and resources needed to restore the disrupted systems or business.

|  |
| --- |
| **Instructions**: *Remove if not true for your company.* As data is stored in the cloud, users should be able to access files anywhere with a secure internet connection.  In the event that a disaster affects the data warehouses where data is stored in the cloud, a backup instance of our data should be created and recoverable through the third-party backup provider **Instructions**: *Insert provider’s name*.  **Instructions**: *Customize calendar details for your company*. The day-to-day calendar stored in the Redtail CRM site can be sync’d with an Outlook calendar providing tactical operational continuation in the event we lose connection to our primary financial portal (Redtail).  **Instructions**: *Remove if not true for your company*. M365 keeps backups of any SharePoint sites and OneDrive files. Additionally, a separate backup to a physical location occurs nightly. |

# Recovery Plan Practice and Exercising

This is the plan that should be carried out to practice and prepare for an emergency.

|  |
| --- |
| Practice of disaster recovery plan:  Scenario: Office internet is down and building suspects internet service will not be restored in a few days.   1. Confirm the main office location cannot connect to the office internet. 2. Direct employees to work from **Instructions**: *Insert “home” or “designated remote work site”* until office internet is restored. IT contact will keep in touch with building management for latest updates. 3. System access to business-critical functions should be available with a secure internet connection. 4. Any applications that are geo-locked or IP-restricted will need to be notified; this will fall to the IT contact to implement. 5. Once office internet is restored and confirmed functional, employees are able to return to the office for normal business operations.   Scenario: Microsoft servers are down and access is unavailable.   1. IT contact should confirm access to Microsoft servers are unavailable. 2. IT contact will access backup files from the third-party backup service provider. 3. IT contact will confirm users have access to data and are able to continue normal business activities.   Exercise of disaster recovery plan:   1. **Instructions**: *Remove if a backup connection is not set up for your company*. Temporarily disable main internet connection. IT contact to confirm that the backup internet connection is available for use. 2. Access the backup data from third-party backup service provider to confirm its availability. 3. Once internet connectivity is available, confirm that employees are able to access business critical systems.   - **Instructions**: *Customize with your company’s systems*.  - Microsoft Teams  - Redtail  - Outlook  - Orion  - QuickBooks  -Custodian sites  - Any other critical systems; this list is not exhaustive and is provided as an example.   1. Confirm that phone lines are operational. Phones should be able to dial out and receive calls. 2. Note any issues or additional steps needed to be taken and update this recovery plan. |

# Disaster Site Rebuilding

These are the steps and resources needed in order to rebuild the disaster site.

|  |
| --- |
| Any changes to the building/home office location will be at the discretion of the building’s property manager and/or property owner. |

# Plan Changes or Updates

These are the details regarding any changes or updates made to the DRP, version number, and history.

|  |
| --- |
| This disaster recovery plan is to be reviewed annually or on an as need basis to adhere to industry standards and industry best practices. This plan is not all inclusive and may require additional sections to be added for specific events. These changes are to be documented and approved by a member of the management team. |