RPAG Business Continuity Plan Overview

GL-IT-10006

Category
Information Technology

Policy Owner
Jami Chapman
Chief Operating Officer

Adopted
7/6/2016

Revised and/or Approved
05/15/2023

Review Frequency
Annually

Related Policies
All RPAG IT Policies

Country/Countries
Global

Attestation Notation:
N/A

Additional Notes:
N/A

Scope

The Business Continuity Plan identifies actions, responsibilities, and contact personnel in the event of a disaster or other interruption of business operations of Retirement Plan Advisory Group ("RPAG"). The Plan seeks to safeguard employees' lives and firm property; evaluate the situation and initiate appropriate action; recover and resume operations for continuation of business; and provide clients with access for their insurance, retirement plan and wealth management needs during such events. The Plan was developed considering the types of business conducted, systems critical to support business, and geographic dispersion of offices and personnel of RPAG. This Plan is current as of the date noted above and may be updated from time to time.

Policy

General Overview

This document provides the basic guidelines for RPAG's Business Continuity Plan ("BCP" or "Plan"). It is intended to serve as a comprehensive BCP for all RPAG offices; however, certain offices may develop and maintain additional policies, procedures and processes tailored to the specific requirements of their locations. The purpose of this document is to aid in the continuation of business and services to our clients in the event or occurrence of a disaster, or other business interruption, affecting the operations of RPAG offices.

This BCP will help enable staff working in an RPAG office to provide critical services and products that must be delivered to ensure continuity of business operations, avoid causing damage or injury to the company and its employees, and help meet legal/regulatory and client obligations of the organization during such times. The BCP is driven by a proactive process to help ensure critical services and products can be delivered during a disruption.

The BCP also assists in the recovery of our facilities, data, operations and assets. The Plan identifies necessary resources to support business continuity, including personnel, information, equipment, financial resources, infrastructure protection, and legal and regulatory requirements.

The BCP contemplates procedures for response and recovery in the event of a significant business disruption. A key part of the Plan is to identify responsible personnel in the event of a disaster; safeguard employees' lives and firm property; evaluate the situation and initiate appropriate action; recover and resume operations to allow continuation of business; continue servicing clients; and protect our data and records. The Plan was developed with consideration to the types of business conducted, systems critical to support business, and geographic dispersion of offices and personnel.

RPAG is committed in planning and preparing itself for the possibility of an event that might cause interruption in its business so that there will the minimum amount of down time and disruption to our clients, employees, firm and offices.

Business Impact

In our fast paced and complex business environment, many types of events might cause an interruption of services. These events can include natural disasters, accidents, power and/or communication interruptions, sabotage/terrorism/cyber-attacks, technology systems failures, epidemics and pandemics, or medical

emergencies. Maintaining the Plan helps RPAG to procure the resources and information needed to deal with these emergencies in the event that they occur.

Each type of emergency or disaster comes with its own unique characteristics and challenges, with differing risks based upon the actual situation. While some events may only cause minor disruptions and can be resolved in a short period with minimal impact, other events or combinations of events might take place over prolonged periods and could cause long-term disruptions.

Business Continuity Plan Guidelines

On a continuous basis, RPAG tries to mitigate its risk to reduce the impact of disasters that might affect its business operations. Some of the key guidelines and functions common for any event are:

- Employee safety - RPAG places emphasis on the safety of its employees by communicating to and training its employees on safety and evacuation procedures.

- Employee BCP training – Key employees are kept current and trained on what action steps might be necessary in the event of business interruption disaster.

- Backup power and data – RPAG has onsite generators at corporate locations with electrical power to operate its critical corporate IT systems and to back up data on a regular basis.

- Separate sites and working from home – In the event of a major disaster, RPAG has offices across the country that will act as backup facilities for RPAG locations that are impacted by a disaster. In addition, nearly all RPAG employees are able to work remotely.

- Most RPAG systems are redundantly hosted in the cloud; consequently, in the event of a disaster, the accessibility, reliability and accuracy of key business systems should not be impacted and can be accessible from alternate, non-impacted areas.

- RPAG works with key third party providers to confirm that such third parties have BCPs in place to cover their systems, operations and personnel.

Designation of Responsibilities

The following is a list of those responsible for the Firm's Business Continuity Plan.

Responsibility	Names or Titles
Maintain, revise and update Plan	BCP Coordination Committee (Chief Operating Officer, Chief Relations Officer, Chief Investment Officer, and Chief Compliance Officer)
Approve Plan	COO
Annual review and testing of Plan	BCP Coordination Committee

Implementation of Plan when a disruption occurs	Emergency Response Team (TBD at time of disruption, based on the nature of the disruption. For example, in 2020, RPAG formed the RPAG Coronavirus Critical Response Team (RPAG CCRT), made up of department heads and business leaders, which meets daily to monitor and respond to changing dynamics using an updated daily task list.)
Maintain, perform quarterly review of, and distribute Emergency Contact List	Head of Human Resources
Post Plan disclosure on applicable firm's web site and update, as required (if needed)	Chief Operating Officer
Review critical third-party assurances of disaster plans or plan summaries: At initial engagement of third party Annually, when this Plan is reviewed As needed, during an applicable disaster	BCP Coordination Committee

Retention and Location of the Plan

Copies of the current version of the Plan are maintained as follows. Copies are dated as of the effective date of the version of the Plan.

- A current hard copy is retained by IT Compliance with a record of a senior manager's approval.

- The Chief Operating Officer and IT Compliance maintain an electronic copy of the Plan for testing and distribution purposes.

- Backup copies are retained electronically by our third party provider in two separate locations.

- Backup copies of the Plan are also retained by the BCP Coordination Committee, as well members of RPAG executive management.

Emergency Contact List

RPAG has established an Emergency Contact List ("List") that includes the names, phone numbers (work and personal lines), email addresses, and other contact information for individuals critical to the firm's business including key employees, key vendors or service providers, regulators, insurance carriers, banks, attorneys, and

other key contacts. The List is provided to key personnel as necessary. The List is reviewed and updated regularly.

Computers

Computer assets and hardware will be managed and leveraged from our third party provider's New York/Austin Corporate offices, nearby RPAG offices, or procured locally as need be.

Alternative Business Locations

In the event employees can no longer conduct business at one of RPAG's office locations, the following actions may be taken:

- Transfer employees to the closest unaffected office location and notify personnel.

- Institute work remote or work from home protocols for employees (as necessary).

- Transfer critical systems to another office or a back-up firm or system.

- Transfer business operations to another firm office unaffected by the disruption.

- Transfer corporate business and operations between the New York and Austin headquarter offices.

Data Back-Up and Recovery

RPAG maintains its data and records in both on and offsite repositories.

In the event of an internal or external significant business disruption that causes the loss of data and records (whether hard copy or electronic records), backup records and data will be recovered from the back-up site(s).

Mission Critical Systems

Mission critical systems are systems that are necessary to ensure prompt and accurate client servicing.

The Plan requires review, identification of, and procedures for those systems that are critical to the operation of our business, including identification of (i) third parties and contacts that provide those systems; and (ii) potential alternate procedures or systems for handling these critical functions in the case of a disruption.

Corporate and Field Communications

RPAG has put in place several mechanisms to be used to communicate with RPAG employees in the event that an unforeseen business interruption occurs. Example of such interruptions and applicable RPAG contacts to send communication and updates are set forth below, along with common communication techniques RPAG may deploy during a given disaster.

Technical Outage:

- Primary: RPAG Relations Officer

- Secondary: Chief Operating Officer

Significant Business Disruption:

- Primary: Head of Human Resources

- Secondary: Chief Relations Officer

Significant Business Disruption for RPAG field offices:

- Primary: Chief Operating Officer

- Secondary: Head of Human Resources

Email

RPAG Technology and Marketing staff have the ability to send email to all email groups. Communications can be sent to RPAG firms via multiple distribution lists and to RPAG clients through multiple distribution lists maintained by the individual firms. In addition, specific email groups and addresses may be established from time to time to correspond to a given disaster to coordinate questions and requests.

Phone Services

Most locations use VoIP phone solutions. In the event of an onsite disaster, telephone service can quickly be re-established to a new location with minimal effort. Each individual using VoIP phone solutions has the ability to forward their number to another number, typically a mobile phone, to continue to receive calls. Each location is also programmed with an emergency option which when enabled will forward all calls to the office to a specific number.

In the event the office is not on VoIP, RPAG can initiate activities with the phone carrier to have phone lines transferred to another non-impacted office or one of RPAG's corporate offices.

Telephone Hotline Recording

As necessary, hotlines or other general phone lines will be established for employees for a given disaster.

Website Message Posting

In addition to the telephone hotline, a message will be posted and updated as often as necessary on the main page, or other landing pages, of RPAG's website (www.rpag.com). RPAG representatives and their clients should be instructed to visit this website for updated information on impacts, responses and closures during a given disaster. The Web site posting should include the date and time of the posting as well as a concise and clear message based on the content approved for mass communication. The website posting will be coordinated by RPAG Technology based on a message prepared by RPAG Marketing.

Secured Off-Site/Cloud Warehousing of Data

Because a fail-safe system is necessary to access critical field communications data from a remote location (e.g., email lists, telephone rosters, etc.) if an office shutdown occurs, all of this data will be stored and secured via cloud and/or tape backup.

Education of Employees

The Plan is communicated to employees as follows:

- A current copy of the Plan is provided to key employees with responsibilities for aspects of the Plan.

- The most recent Emergency Contact List is provided to key employees.

- A copy of the Plan is made available internally to all employees on systems and resources.

Updating, Annual Review, and Testing

The Plan will be reviewed and revised annually and as needed. Each revision will be approved by a designated senior manager and copies of the revised Plan distributed to key employees. Some material events require updating the Plan when they occur, including:

- Material changes to the firm's business.

- A change in the firm's main office location.

- Added office locations.

- A change in a major service provider.

- An actual disaster occurring for which this Plan is implemented.

Testing will be conducted at minimum annually, and a summary report will be produced at the conclusion of testing.

Definitions

- **Terms:** N/A