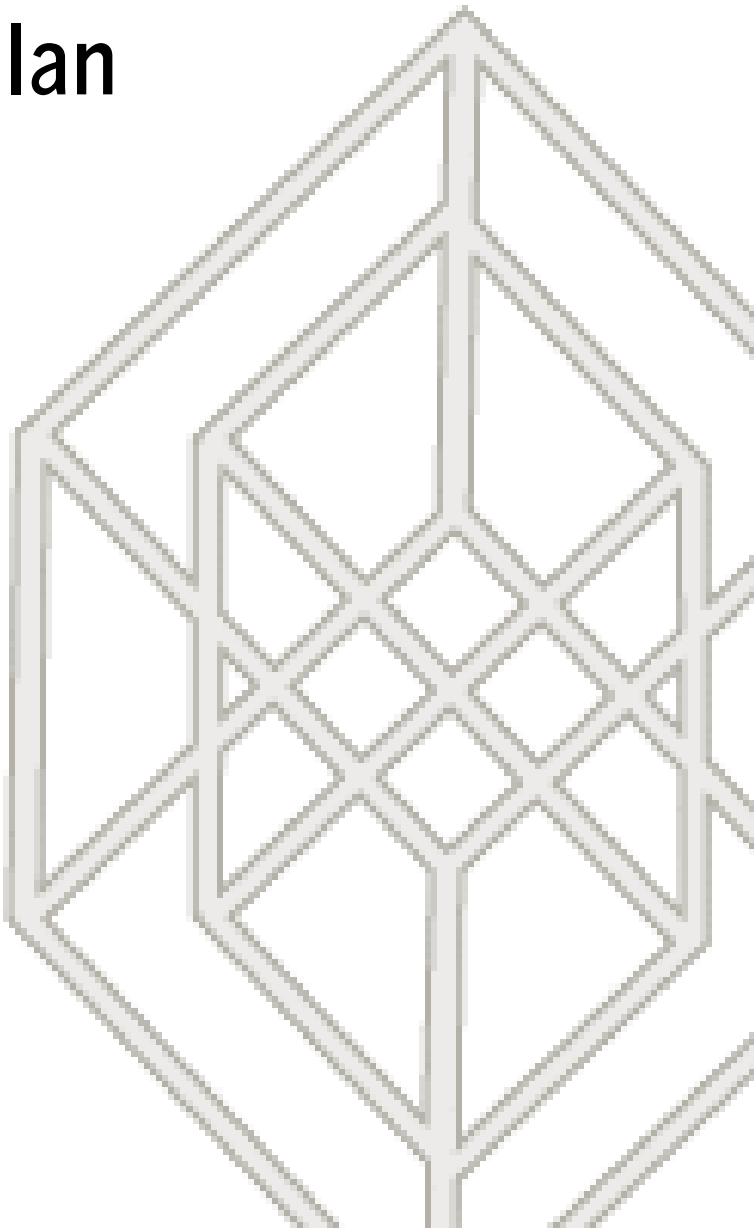
Paul Consulting Group

Hosting Disaster Recovery / Continuing Operations Communications Plan

Last Reviewed:
March 2024



Overview

The Paul Consulting Group *(hereinafter "PCG")* disaster recovery plan covers the hardware, software, and data critical for PCG to restart operations in the unlikely event of a natural or human-caused disaster. The Plan is intended to ensure that, in the event of a crisis, disaster, or emergency related to PCG clients, equipment, or systems, information about the crisis and the action taken is disseminated appropriately, accurately, and clearly.

Emergency: Any situation that may involve or threaten to cause equipment, hardware, software and data, or service failure.

Non-Emergency: Any situation that threatens the reputation of PCG, loss of key management, or poses legal ramifications, but does not pose a direct physical threat to employees, clients, or services.

Plan Instructions

PCG will keep a copy of this plan both at the office and offsite. A copy of the plan will also be maintained offsite both electronically and in paper format. It is the responsibility of PCG leadership to ensure that a copy of the plan is available to each team member, other staff and key emergency response partners for use in the event of a crisis. It is also the responsibility of the PCG leadership team to ensure that the plan is kept up-to-date and that the team members have read the plan and understand its contents.

Plan Review

The PCG leadership team will review this plan on a bi-yearly basis to check that:

- Contact information lists are current.
- New initiatives or identified risks are assessed and included.
- Changes to risk communications policies, practices or procedures are up-to-date.

Spokesperson

During an emergency, the President or Vice President of Technology (or another designee) will serve as the PCG's spokesperson.

Other PCG staff will refer inquiries to spokesperson.

Response

1. Verify the Crisis Situation

PCG leadership will meet promptly to determine what has happened (what, when, who, how, why), identifying as many facts as possible.

- WHAT happened and where?
- WHEN did this happen?
- WHO is involved?
- HOW did it happen?
- WHAT is currently being done?

2. Notification and Assignments

Communication notifications steps:

1. Notification is made to President (or assigned designee) within 15 minutes of incident.
2. President should immediately call the Crisis Team Lead.
3. A meeting should take place with the Crisis Team for briefing and determine next steps.
4. If meeting space is not available, phone calls should be made.

Crisis Team Assignments:

Role/Responsibility	Primary Name	Alternate Name
<u>Crisis Team Leader</u> • Coordinates PCG communication response • Oversees message development and coordinates message with external partners if necessary (i.e. colo) • Final approval of all publicly disseminated information. • Arranges scheduled and emergency team meetings. • Oversees broad and specific team functions. • Ensures required resources are available for team member assigned duties. • Communicates with external partners	Ryan Brooks	Marc Paul
<u>Assistant CCT Coordinator</u> • Assists the team coordinator with prioritizing duties and handling inquiries. • Fulfills all the duties and responsibilities of the CTL his/her absence. • Works in close liaison with the spokesperson facilitator to ensure message accuracy.	Drew Perkins	
<u>Spokesperson</u> • Spokesperson	Marc Paul	

• Assists the CTL with prioritizing duties. • Provide communication input. • Serves as lead PCG representative		

Communication Management, Development, and Release

Message Management

1. Schedule regular internal communication updates.
2. Schedule regular updates with external partners if necessary.
3. Identify key audiences.
4. Identify main contact with external partners.

Message Development

Once the information to be communicated has been confirmed, it is time to begin planning a response strategy for communicating critical information and for responding to potential questions.

1. Develop a script for conveying key information points.
2. Develop or refer to a list of questions that could be asked by a variety of audiences (clients, partner, organizations) about the crisis.
3. Develop messages.
4. Identify the best methods for delivery of key messages.
5. Monitor crisis and update messages based on the crisis.

Release Messages

Messages sent to PCG Hosting Clients can be sent using the distribution list titled “PCGHosting” in Outlook. The PCG Hosting distribution list includes all PCG staff.

Resource A: Equipment Outage

In the event of equipment outage, an assessment of the damage is made to determine the estimated length of the outage. If the outage is estimated to be less than twelve hours’ normal procedures will be applied to restore the affected service(s) to full operational status. If the outage is estimated at longer than twelve hours, then the Vice President of Technology is notified of the event and the plan then enters the backup stage.

In the event of a prolonged and total outage of more than twenty-four hours, critical service(s) as noted in Resource C are resumed first from an initial backup server. The backup server will support all critical service(s), possibly in a degraded state, until the affected server(s) can be brought back online.

If the affected server(s) cannot be restored to fully operational status due to catastrophic damage then alternate equipment will be accrued and installed to restore full service.

If loss of critical data deemed necessary to provide a full service, as set out in the PCG Hosting Terms & Conditions, has occurred due to the disaster then off-site backups will be restored within seventy-two hours at our disaster recovery destination. Please refer to the developer wiki information at https://devwiki.paulconsulting.com for further Disaster Recovery instructions.

Once full recovery has been completed, an internal investigation into the cause and impact of the disaster will be undertaken. The report will contain an appraisal of our response to the Disaster and any steps that can be taken to reduce the impact of any similar disasters in the future.

Sample messaging is available under Resource I (Resource is only available for PCG staff).

Resource B: Location

PCG customer webserver and database server are in a Tier IV datacenter. This facility has limited access and is monitored with security systems, fire / temperature notifications, generators, and battery backups.

The EdgeConnex building is located at:

EdgeConnex
1531 Commonwealth Business Drive
Tallahassee, FL 32303
Phone: +1 (866) 304-3217

The offsite disaster recovery company PCG utilizes is:

Microsoft Azure under the Paul Consulting Group tenant

Resource C: Critical Services

Services deemed critical to provide service set out in our Terms & Conditions:

- DNS service
- E-mail service, including:
  - SMTP
  - Forwarding Services
- Hosting service, including:
  - IP Bindings
  - SFTP
  - SQL Databases
  - Web services (APIs)
  - SSL

Resource D: Critical Data

Data deemed critical to provide service set out in our Terms & Conditions:

- DNS configurations
- Domain settings
- E-mail settings
- Website (www) configurations
- Bound IP's
- Webserver & Data Server Backups
- Firewall settings
- SSL certificate data
- Server configurations
- Spam dictionaries

Considerations for PCG Clients

The responsibility of client data stored and served by any PCG service remains the client's sole responsibility and property at all times. We advise all members to maintain their own Disaster Recovery Plan and to take periodic backups of their own data.

Resource E: Additional Information

For additional information and resources related to hosting, please refer to:
https://www.paulconsultinggroup.com/managedhosting