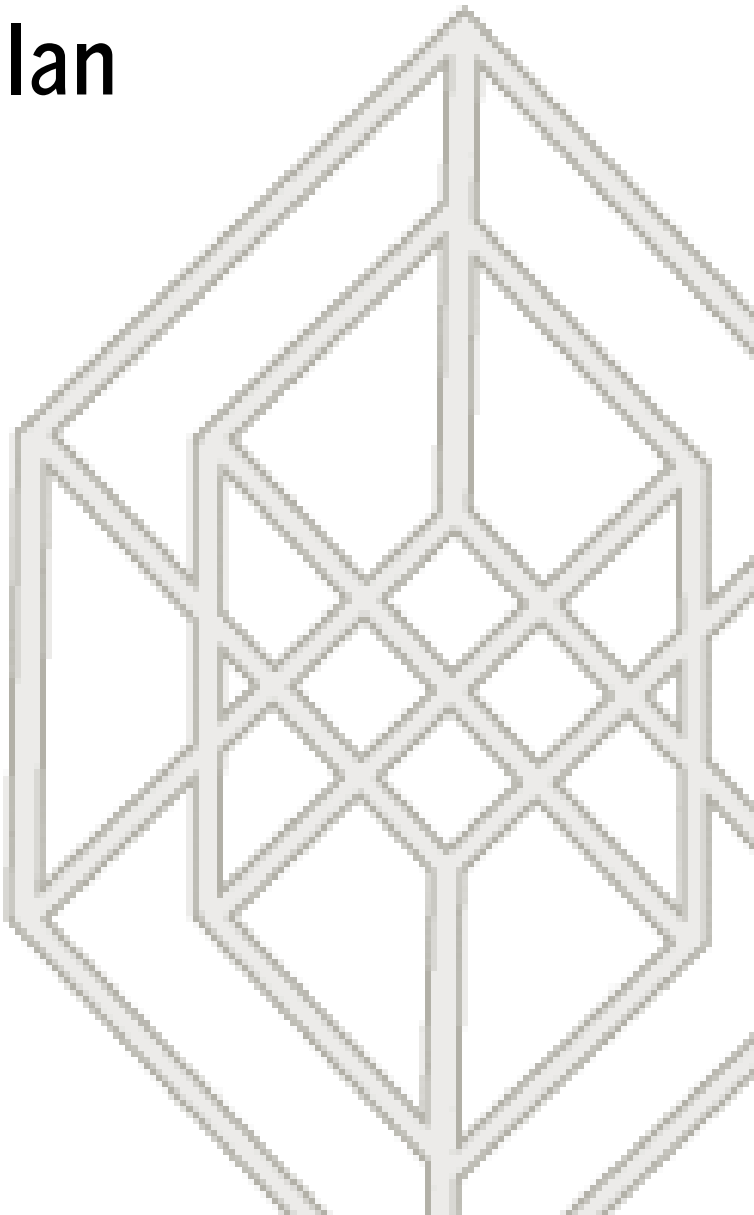
Paul Consulting Group

Hosting Disaster Recovery / Continuing Operations Communications Plan

Last Reviewed:
August 2026



Overview

This disaster recovery and continuing operations plan describes how Paul Consulting Group (PCG) prepares for, responds to, communicates during, and recovers from events that affect its managed hosting services. It covers the people, facilities, hardware, software, data, communications, backups, and recovery resources required to restore critical services following a natural disaster, technology failure, cyber incident, or other disruptive event.

The objectives of this plan are to:

- Protect customer data and PCG-managed systems.
- Restore critical hosting services in accordance with applicable customer agreements and service-specific recovery objectives.
- Provide timely, accurate communications to customers, employees, and external partners.
- Document lessons learned and corrective actions following an incident.

Emergency: An event that has caused, or is likely to cause, an interruption to hosted services, equipment, software, data, communications, or facility operations.

Non-emergency: An event that may affect PCG's reputation, legal obligations, management availability, or business operations without immediately interrupting hosted services.

Plan Availability and Maintenance

PCG maintains copies of this plan in secure onsite and offsite locations. PCG leadership is responsible for ensuring that authorized personnel can access the plan during an incident and that assigned team members understand their responsibilities.

The plan is reviewed semiannually and following any material incident or infrastructure change. Each review confirms that:

- Contact information and team assignments are current.
- Infrastructure, backup, monitoring, and recovery procedures reflect the current environment.
- New services, risks, dependencies, and regulatory requirements have been considered.
- Communication and escalation procedures remain appropriate.
- Results from recovery exercises and actual incidents have been incorporated.

Roles and Responsibilities

Crisis Team Leader

The Crisis Team Leader coordinates the overall response, establishes priorities, convenes the Crisis Team, confirms that required resources are available, coordinates with external partners, and approves customer-facing communications.

Assistant Crisis Team Coordinator

The Assistant Crisis Team Coordinator supports incident coordination, manages assigned response activities, and performs the Crisis Team Leader's responsibilities when necessary.

Spokesperson

The President, CIO, or an assigned designee serves as PCG's spokesperson. Other PCG personnel refer external inquiries to the designated spokesperson.

Incident Response and Escalation

1. Verify and assess the incident

PCG personnel will promptly determine:

- What happened and which systems, customers, or locations are affected.
- When the incident began and whether it is ongoing.
- Who is involved in the response.
- The probable cause, when known.
- What containment, restoration, or recovery actions are underway.
- The estimated duration and business impact.

2. Notify and assemble the Crisis Team

1. Notify the President, CIO, or assigned designee within 15 minutes of confirming a significant incident.
2. Notify the Crisis Team Leader and required technical personnel.
3. Establish a meeting or conference call to review impact, priorities, responsibilities, and communication requirements.
4. Engage relevant external partners, including Cologix, Microsoft Azure, Internet service providers, and other vendors, when required.

3. Contain, restore, or activate disaster recovery

Technical personnel will begin containment and restoration immediately. The Crisis Team Leader and CIO will determine whether to activate disaster recovery based on:

- The scope and expected duration of the incident.
- The availability of the primary Cologix environment.
- The condition of production data, backups, and recovery systems.
- Customer-specific recovery objectives and contractual commitments.
- Whether recovery in Microsoft Azure will restore service more quickly or reduce risk.

Disaster recovery activation is based on incident conditions and service-specific recovery objectives; there is no mandatory waiting period before recovery actions may begin.

4. Communicate and monitor

PCG will provide updates at a frequency appropriate to the incident. Communications will identify the known impact, actions underway, expected next update, and any required customer action. Information will be verified before release and updated as conditions change.

5. Complete recovery and review

Following restoration, PCG will validate service operation, monitor for recurrence, and complete an internal review. The review will document the cause and impact of the incident, the effectiveness of the response, lessons learned, and corrective actions.

Communication Management

During an incident, PCG will:

- Identify affected customers, employees, vendors, and other stakeholders.
- Assign a primary contact for each external partner.
- Prepare clear messages using confirmed information.
- Schedule internal and external updates appropriate to the severity of the incident.
- Track customer questions and required follow-up actions.
- Maintain a record of significant decisions and communications.

Customer messages may be distributed through PCG's approved hosting-client distribution lists or other established communication channels.

Resource A: Equipment or Service Outage

PCG will promptly assess an outage and begin restoration using the safest and fastest appropriate method. Depending on the affected service, recovery may include:

- Failing over clustered services within the primary environment.
- Restoring a virtual machine, application, database, or configuration from an onsite backup.
- Recovering from an offsite backup stored in Microsoft Azure.
- Activating disaster recovery web and database systems in Microsoft Azure.
- Replacing failed equipment or obtaining alternate equipment when restoration is not practical.

Service-specific recovery objectives and customer commitments take precedence over general planning estimates. Detailed technical recovery procedures are maintained internally and are available only to authorized PCG personnel.

After recovery, PCG will investigate the incident and identify measures that may reduce the likelihood or impact of similar events.

Resource B: Hosting and Disaster Recovery Locations

Primary hosting location

Cologix JAX2
4800 Spring Park Road
Jacksonville, FL 32207
Phone: (855) 265-6449

Disaster recovery location

Microsoft Azure
PCG-managed Azure tenant

PCG's primary managed-hosting systems operate at Cologix JAX2. Microsoft Azure provides offsite backup storage and disaster recovery infrastructure. Recovery methods vary by hosted service and may include encrypted Veeam backup copies, application file synchronization, SQL Server transaction log shipping, and preconfigured disaster recovery virtual machines.

Resource C: Critical Services

Critical services may include:

- DNS and domain configuration services.
- Web applications and websites.

- Web services and APIs.
- SQL Server databases.
- SSL/TLS certificates and bindings.
- Secure file-transfer services.
- Email-related services when included in a customer's hosting agreement.
- Firewall, routing, and required network services.

Restoration priority is determined by safety, business impact, system dependencies, customer commitments, and the scope of the incident.

Resource D: Critical Data and Configuration

Critical data and configuration may include:

- DNS and domain configurations.
- Website and application files.
- SQL Server databases and transaction logs.
- Virtual-machine and server backups.
- Firewall, routing, and security configurations.
- SSL/TLS certificates and related configuration.
- Server, application, and monitoring configurations.
- IP bindings and secure file-transfer configurations.
- Other customer data covered by an applicable hosting agreement.

Customer Data and Shared Responsibility

Customer data remains the property of the customer. PCG protects and recovers PCG-managed hosting systems and data in accordance with applicable agreements, documented backup practices, and service-specific recovery procedures. Customers remain responsible for their own business continuity planning, user access, application use, and any backup or export responsibilities assigned to them by contract. PCG recommends that customers maintain an independent business continuity plan appropriate to their operations.

Backup and Ransomware Protection Summary

- Veeam backup-file encryption is enabled for managed backup jobs.
- Onsite backup copies are stored in a dedicated, restricted SAN volume at Cologix.
- Offsite backup copies are stored separately in Microsoft Azure Blob Storage.
- Backup encryption credentials are maintained in a restricted password vault.
- Backup jobs are monitored and failures are investigated.
- Deleting all backup copies requires access to both the onsite backup environment and the separately administered Azure environment.
- The current Azure object-storage repository is not immutable. PCG plans to implement immutable Azure object storage during Q4 2026 through Q1 2027.

Additional Information

Additional information about PCG managed hosting is available at:

https://www.paulconsultinggroup.com/managedhosting