Business Continuity and Disaster Recovery (BC/DR)

Policy Owner: Security Team

Effective Date: 2/26/2025

Purpose

The purpose of this business continuity plan is to prepare Power Digital in the event of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible in a minimum time frame.

Scope

All Power Digital IT systems that are business critical. This policy applies to all employees of Power Digital and to all relevant external parties, including but not limited to Power Digital consultants and contractors.

1. Policy

In the event of a major disruption to production services and a disaster affecting the availability and/or security of the Power Digital office, senior managers and executive staff shall determine mitigation actions.

A disaster recovery test, including a test of backup restoration processes, shall be performed on an annual basis.

Continuity of information security shall be considered along with operational continuity.

In the case of an information security event or incident, refer to the Incident Response Plan.

2. Alternate Work Facilities

If the Power Digital office becomes unavailable due to a disaster, all staff shall work remotely from their homes or any safe location.

3. Communications and Escalation

Executive staff and senior managers should be notified of any disaster affecting Power Digital facilities or operations.

Communications shall take place over any available regular channels including ; Slack Channels, Zoom meetings, or email communications.

Key contacts shall be maintained on the on-call schedule and key contacts

Roles and Responsibilities

Role	Responsibility
Departmental Heads	Each department head shall be responsible for communications with their departmental staff and any actions needed to maintain continuity of their business functions. Departmental heads shall communicate regularly with executive staff and the IT Manager.
Managers	Managers shall be responsible for communicating with their direct reports and providing any needed assistance for staff to continue working from alternative locations.
CEO	The CEO shall be responsible for any external and client communications regarding any disaster or business continuity actions that are relevant to customers and third parties.
Director of Platform Engineering	The Director of Platform Engineering, in conjunction with the VP of Global Support, shall be responsible for leading efforts to maintain continuity of Power Digital services to customers during a disaster. The Director of Platform Engineerin shall lead BC/DR efforts to mitigate losses and recover the corporate network and information systems.
HR Manager	The HR Manager shall be responsible for internal communications to employees as well as any action needed to maintain physical health and safety of the workforce. The VP of Human Resources shall work with the IT Manager to ensure continuity of physical security at the Power Digital office.

4. Continuity of Critical Services

Procedures for maintaining the continuity of critical services in a disaster can be found in Appendix A.

Strategy for maintaining continuity of services can be seen in the following table:

KEY BUSINESS PROCESS	CONTINUITY STRATEGY
Customer (Production) Service Delivery	Rely on AWS & GCP availability commitments and SLAs
IT Operations	Not dependent on HQ. VPN is redundant between HQ and Colo. Critical data is backed up to alternate locations.
Email	Utilize GSuite and its distributed nature, and rely on GSuite standard service level agreements.
Finance, Legal and HR	All systems are vendor-hosted SaaS applications.
Sales and Marketing	All systems are vendor-hosted SaaS applications.

Plan Activation

This BC/DR shall be automatically activated in the event of the loss or unavailability of the Power Digital office, or a natural disaster (i.e., severe weather, regional power outage, earthquake) affecting the larger San Diego, United States region.

Version	Date	Description	Author	Approved by
1.0	5/10/2024	First Version	Security Team	John Taumoepeau
2.0	2/25/2025	Second Version	Security Team	Javier Garcia

Appendix A – Business Continuity Procedures by Scenario

Business Continuity Scenarios

Hosting Provider Outage

- Contact On Call Engineers, and Director of Platform Engineering
- Contact IaaS provider support team to obtain details
- Verify the components the outage impacts (All components, databases, servers, etc)
- Publish application status on status page or send mass communication to customers with an estimated timeline on recovery
- Communicate outage status with internal employees

Internal Tool Outages (Email, Slack, Conference Tools)

- Contact SaaS providers and obtain details on estimated recovery time.
- Communicate outage details to employees
- Confirm impact to customer data and operations that may impact customers
- Communicate outage details to customers with estimated recovery time if the outage impacts customers

Appendix B – Recovery Objectives and Procedures

Recovery Point Objective (RPO)

Definition

The RPO is the maximum tolerable period in which data might be lost due to a major incident. It defines the acceptable amount of data loss measured in time.

Objective

Power Digital aims to limit data loss to no more than 24 hours. All critical systems must ensure daily backups to meet this objective.

Details

- **Customer Data**: Data should be backed up daily with a retention period of one month.
- **Operational Data:** All operational data, including system logs, should have a backup frequency that does not exceed 24 hours.
- **Financial Data:** Financial data should be backed up every 12 hours to ensure minimum disruption to financial operations.

Recovery Time Objective (RTO)

Definition

The RTO is the maximum acceptable length of time that a system can be offline following a disaster.

Objective

Power Digital aims to recover critical systems and resume business operations within 4 hours of a disruption.

Details

- **Priority 1 Systems**: These are systems critical to customer service and operational continuity, such as the Customer Relationship Management (CRM) and email servers, which must be restored within 2 hours.
- **Priority 2 Systems:** These systems, including internal communication tools and file servers, must be restored within 4 hours.
- **Priority 3 Systems**: Non-critical systems like internal documentation and lesser-used applications should be restored within 24 hours.

Detailed RPO and RTO Table:

System/Service	RPO	RTO	Notes
CRM	12 hours	2 hours	Critical for customer interaction
Email Server	24 hours	4 hours	Essential for internal/external communication
Financial System	12 hours	4 hours	Critical for financial operations
Website	24 hours	2 hours	Crucial for customer access
Internal Tools	24 hours	4 hours	Important for internal operations
File Servers	24 hours	24 hours	Non-critical data storage

Detailed Disaster Recovery Procedures

Step-by-Step Recovery Process

Outline specific steps for restoring services and systems after a disruption.

Roles and Responsibilities

Clearly define who is responsible for each step in the recovery process.

- Checklists: Provide checklists for key tasks to ensure all necessary actions are taken during recovery.

Data Backup and Restoration

Backup Locations

Specify where backups are stored (e.g., cloud storage, offsite facilities).

Backup Frequency

Detail the frequency of backups for different types of data (daily, weekly, etc.).

Backup Verification

Outline procedures for regularly testing and verifying backups to ensure data integrity.

Critical Systems and Data Inventory

System Inventory

List all critical systems and their dependencies.

Data Inventor

Detail the types of data stored in each system and their importance to business operations.

Recovery Priority

Identify which systems and data should be recovered first based on business impact.

Communication Plan

Internal Communication

Define protocols for informing employees and management during a disaster.

External Communication

Provide guidelines for communicating with customers, partners, and stakeholders.

Contact Information

Include an updated list of key contacts, including IT staff, vendors, and emergency services.

Vendor and Supplier Coordination

Vendor Contact Information

List contact details for critical vendors and suppliers.

Service Level Agreements (SLAs)

Summarize key SLAs with vendors that support disaster recovery.

Coordination Procedures

Outline steps for coordinating with vendors during recovery efforts.

Recovery Site Information

Alternate Work Locations

Detail alternate sites for operations if the primary site is unusable.

Access and Security

Provide procedures for accessing recovery sites and ensuring security.

- Equipment and Resources: List essential equipment and resources available at recovery sites.

Testing and Maintenance

Test Schedules

Establish a schedule for regular testing of the disaster recovery plan.

Test Scenarios

Describe various scenarios to be tested (e.g., data center failure, cyber-attack).

- Review and Updates: Specify procedures for reviewing test results and updating the recovery plan.

Incident Response Procedures

- Incident Identification: Detail how to identify and classify different types of incidents.

- Immediate Actions: Provide initial steps to take when an incident occurs to mitigate impact.

- Escalation Paths: Define escalation procedures for incidents that require higher-level intervention.

Compliance and Legal Considerations

Regulatory Requirements

List relevant regulatory requirements that the recovery plan must comply with.

- Data Protection Laws

Outline data protection and privacy laws that affect the recovery process.

Reporting Obligation

Identify any reporting requirements to authorities or stakeholders in the event of a disaster.

Training and Awareness

Employee Training

Detail training programs for employees on their roles in disaster recovery.

- Awareness Programs: Outline programs to increase awareness of the recovery plan and its importance.

Documentation Access

Ensure employees know where to find recovery plan documents and resources.

Insurance and Financial Recovery

Insurance Coverage

Provide details of insurance policies that cover business interruptions and recovery.

Claim Procedures

Outline steps for filing claims and the documentation required.

- Financial Contingencies: Include plans for financial support during recovery, such as emergency funds or lines of credit.

Recovery Metrics and Reporting

Key Metrics

Define metrics to measure the effectiveness of the recovery plan (e.g., downtime, data loss).

Reporting Procedures

Outline procedures for reporting recovery status to management and stakeholders.

Continuous Improvement

Include processes for reviewing and improving the recovery plan based on performance metrics.