SECURITY

Business Continuity and Disaster Recovery (BC/DR) Policy

Policy Owner: Paul Jones

Version: 2.2

Effective Date: 2021-07-06

Last Reviewed: 2026-02-24

1. Purpose

To ensure the continued availability of critical systems and services and to define recovery strategies in the event of regional, infrastructure, or operational disruptions affecting Crystal Project Inc.

2. Scope

This policy applies to:

- Production systems and infrastructure
- Customer-facing services
- Critical internal business systems
- Backup and recovery processes

Crystal Project Inc. operates as a fully remote organization and does not rely on physical office infrastructure for core business continuity.

3. Resilience Architecture

Production systems are designed for high availability within a primary AWS region.

Continuity controls include:

- Multi-Availability Zone (multi-AZ) deployment within the primary AWS region
- Automated failover at the availability zone level

- Infrastructure-as-code configuration management enabling rapid environment reconstruction
- Redundant managed services where applicable

The primary production database is deployed in a multi-AZ configuration. In the event of an availability zone failure, automated promotion of a standby replica occurs within the same region.

In the event of a regional outage, recovery is achieved through infrastructure redeployment and restoration from backups. Recovery time objectives reflect this approach.

4. Disaster Scenarios

Disruption scenarios considered within scope include:

- Availability zone failure
- Regional cloud service disruption
- Infrastructure misconfiguration
- Data corruption
- Security incidents affecting availability
- Critical SaaS provider outages

Cloud provider outages are within the scope of BC/DR planning and response.

5. Failover and Recovery

Failover procedures are designed to restore services in the event of availability zone or infrastructure disruption.

Recovery mechanisms may include:

- Automated multi-AZ failover within the primary region
- Promotion of standby database replicas
- Infrastructure redeployment via code
- Restoration from backups

Recovery capabilities are validated periodically through restore testing, tabletop exercises, or controlled simulations.

6. Backup and Data Protection

Critical production data is protected through:

- Automated cloud-native backups within the primary AWS region
- Controlled access to backup storage
- Periodic restore validation testing (at least annually)

Recovery point objectives (RPO) depend on the backup frequency and retention configuration at the time of disruption.

7. Recovery Objectives

Recovery objectives are risk-based and prioritize:

- Restoration of customer-facing services
- Protection of data integrity
- Preservation of confidentiality
- Minimization of downtime

Recovery time and recovery point objectives (RTO/RPO) are determined by system criticality and architectural design.

8. Business Operations Continuity

Core business functions rely on distributed SaaS providers (e.g., email, collaboration, CRM, finance).

Personnel operate remotely and are not dependent on centralized facilities.

Business continuity is therefore not tied to a single physical location.

9. Integration with Incident Response

Major availability disruptions are managed in coordination with the Incident Response Policy.

Post-incident reviews are conducted following material outages to identify improvement opportunities.

10. Testing and Review

Disaster recovery readiness is evaluated through:

- Restore testing (at least annually)
- Tabletop exercises
- Architecture review during significant system changes
- Post-incident analysis

This policy is reviewed at least annually.

11. Exceptions

Exceptions must be documented and approved by the Policy Owner.

12. Review and Revision History

Version	Date	Description	Author
1.0	2021-07-06	Initial Version	Jona Morua
2.2	2026-02-24	Updated to reflect active/active multi-region architecture with automated failover	Paul Jones
2.3	2026-06-25	Updated to reflect single-region multi-AZ architecture	Paul Jones