

Business Continuity and Disaster Recovery Policy

Purpose

Disruptions — whether from cyber incident, cloud provider outage, natural disaster, supplier failure, or workforce unavailability — are inevitable. This policy sets Your Organization's expectations for continuing critical business operations and recovering information systems during and after a disruption, and assigns accountability for the plans, tests, and exercises that keep us ready.

Scope

This policy applies to every Your Organization business process and information system. It applies to all workforce members involved in the continuity program — plan owners, system owners, and the leadership who make disruption-time decisions.

Definitions

- **Business Continuity (BC).** The capability to continue delivering products and services at acceptable predefined levels following a disruption.
- **Disaster Recovery (DR).** The technical subset of BC concerned with restoring IT systems and data after a disruption.
- **Recovery Time Objective (RTO).** The target elapsed time between disruption onset and restoration of a service.
- **Recovery Point Objective (RPO).** The maximum acceptable data loss measured as the age of the last recoverable data.
- **Business Impact Analysis (BIA).** Analysis that identifies critical processes, their dependencies, and the impact of disruption over time.

Recovery objectives

Your Organization categorizes systems by criticality using a BIA refreshed at least annually. Each tier carries default recovery objectives; system owners may tighten them based on the BIA but may not loosen them without documented approval.

Tier	Criticality	Default RTO	Default RPO
Tier 1	Mission critical (revenue-bearing customer-facing systems)	4 hours	15 minutes
Tier 2	Important (internal revenue-supporting systems)	24 hours	4 hours
Tier 3	Standard (productivity and back-office systems)	72 hours	24 hours
Tier 4	Deferred (non-critical ancillary systems)	7 days	Best effort

Responsibilities

- **Executive Sponsor.** Approves the BC/DR program, declares disaster when warranted, and owns the strategic decisions during a disruption.
- **BCM Lead.** Accountable for maintaining, testing, and improving the BC/DR program. Coordinates the BIA, plan updates, and exercises.
- **System Owners.** Maintain the DR plan for each system they own, validate that backups and replication work, and participate in exercises.
- **Incident Commander.** During a declared disaster, coordinates tactical response alongside the BCM Lead.
- **Workforce members.** Know their role in the plan for their team and follow communications instructions during a declared event.

Plans and playbooks

Each tier-1 and tier-2 system has a written DR plan that includes: system description and dependencies, RTO and RPO, backup and replication architecture, step-by-step recovery procedure, named responsible roles, communications tree, and a log for exercise results.

The Your Organization business continuity plan includes: declaration criteria, governance during a declared event, communications strategy, workforce safety, alternate work arrangements, and process-level continuity notes for each critical function.

Backups

- Critical data is backed up on a schedule consistent with its tier's RPO.
- Backups are stored in at least one location geographically separate from the primary system.
- Backups are encrypted at rest.
- Backup integrity is verified through restoration tests — the existence of a backup is not sufficient evidence of recoverability.

Testing and exercises

- **Tier 1 systems.** Full DR test at least annually with documented results.
- **Tier 2 systems.** DR test at least every 18 months.
- **Tier 3 and 4 systems.** Tabletop validation at least every 24 months.
- **Company-wide tabletop.** An annual executive-level BC exercise simulating a major disruption (prolonged SaaS outage, regional disaster, or ransomware) and exercising the declaration, communications, and cross-functional decision-making loops.

Exercise findings feed remediation items tracked to closure by the BCM Lead.

Third-party continuity

Critical suppliers (SaaS platforms, payment processors, data center operators, key service providers) are assessed during vendor onboarding for their own BC/DR posture and reviewed at least annually per the Vendor Risk Management Policy.

Scope exceptions

Exceptions must be submitted in writing and approved by the CISO and the Executive Sponsor, document compensating controls, and be time-bound.

Related plans

This policy sets the program's objectives, tiering, and accountability; the operational detail for each of those objectives lives in a dedicated plan so the how does not drift from the what:

- **Business Continuity Plan.** The activation criteria, roles, communications, and return-to-normal procedure this policy's BC objectives require.
- **Disaster Recovery Plan.** The per-tier recovery strategy, RTO/RPO validation, and runbook structure this policy's DR objectives require.
- **Backup Policy.** The 3-2-1, immutability, and restore-testing requirements the RPO commitments in this policy and the Disaster Recovery Plan both depend on.
- **Incident Response Plan.** A security incident that meets this policy's BC/DR activation criteria hands off from incident response to business continuity without waiting for the incident to be fully resolved — the Incident Commander and BCM Lead coordinate the two in parallel. Incident response owns detection, containment, and eradication; this policy's plans own keeping the business running and getting systems back.

Review cadence

This policy and the supporting plans are reviewed annually by the BCM Lead and the Executive Sponsor, or sooner following any significant disruption, material change in Your Organization's technology footprint, or change in regulatory obligations.

Effective date: [the date this policy takes effect]