

# Disaster Recovery Plan

---

## Purpose

This plan defines how Your Organization restores information systems and data after a disruption. It is the technical counterpart to the Business Continuity Plan: where that plan covers people, process, and communications, this plan covers systems, infrastructure, and data. Recovery strategies are organized by the criticality tier each system is assigned in the recovery register (the same tiering the Business Continuity and Disaster Recovery Policy defines) rather than restated here, so a tier's RTO/RPO commitment is defined in exactly one place.

## Scope

This plan applies to every information system in the recovery register, and to the engineering, platform, and vendor personnel responsible for restoring them. It does not cover the business-process-level continuity actions (alternate operations, communications) that the Business Continuity Plan owns.

## Recovery strategies by tier

- **Tier 1 (mission critical).** Active-active or warm-standby architecture where feasible; automated failover with a documented manual fallback. Recovery is validated to the register's Tier 1 RTO/RPO commitments.
- **Tier 2 (important).** Warm or cold standby with documented, rehearsed restoration steps. Recovery is validated to the register's Tier 2 commitments.
- **Tier 3 (standard).** Restoration from backup to newly provisioned infrastructure. Recovery is validated to the register's Tier 3 commitments.
- **Tier 4 (deferred).** Restoration from backup on a best-effort basis once higher tiers are stable.

A system's actual, tested recovery time and point are tracked against its committed RTO/RPO in the recovery register; a gap between the two is a finding, not an acceptable variance, and is tracked to closure by the system owner.

## RTO/RPO commitments

Recovery Time Objective (RTO) and Recovery Point Objective (RPO) targets for every system are maintained in the recovery register, not in this plan, so the plan cannot go stale relative to the register it governs. System owners may tighten their system's commitment; loosening one requires the same documented approval the policy requires.

## Runbook structure

Each Tier 1 and Tier 2 system's DR runbook follows a consistent structure so a responder unfamiliar with a specific system can still execute it under pressure:

1. **System description and dependencies** — what the system does, and what it depends on to come back online (upstream systems, DNS, secrets, network paths).
2. **Declaration trigger** — the specific, observable condition that means this runbook should be started.
3. **Recovery steps** — numbered, unambiguous, and written to be followed by whoever is on call, not only the system's usual owner.
4. **Validation steps** — how the responder confirms the system is actually healthy, not merely running (data integrity checks, smoke tests, a known-good transaction).
5. **Rollback/fallback** — what to do if the primary recovery step fails.
6. **Named roles** — who executes, who validates, who is notified when recovery completes.
7. **Exercise log** — dated results of every test or real execution of this runbook.

## Testing cadence

- **Tier 1 systems.** Full recovery test at least annually, executed against the actual runbook (not a walkthrough), with a written pass/partial/fail result.
- **Tier 2 systems.** Recovery test at least every 18 months.
- **Tier 3 and 4 systems.** Tabletop validation at least every 24 months, verifying the runbook is current even where a full restore is not exercised.

A partial or failed test result opens a remediation item owned by the system owner and is re-tested before the next scheduled cycle, not deferred to it.

## Coordination with the Business Continuity Plan

A disaster declared under this plan that affects a business process in the BIA triggers the Business Continuity Plan's activation criteria; the Incident Commander and BCM Lead coordinate the two efforts so technical recovery and business-side continuity actions run in parallel rather than in sequence.

## Review cadence

This plan is reviewed annually by the BCM Lead and affected system owners, or sooner following a real DR execution, a failed or partial recovery test, or a material change to a Tier 1 or Tier 2 system's architecture.

*Effective date: [the date this policy takes effect]*