

Business Continuity and Disaster Recovery Plan

Owner	[Security owner role]
Approved by	[Policy approver role]
Effective date	[Effective date]
Next review	[Next review date]
Version	[Version]

1. Purpose and scope

This plan sets how [Company name] (the "Company") keeps its service running through a disruption and recovers from one. It supports the SOC 2 common criteria CC7.5 and CC9.1 by establishing recovery activities and risk mitigation for business disruptions.

This plan applies to every critical system within [In-scope systems], and to the people and vendors those systems depend on.

2. Recovery objectives

The Company targets a recovery time objective of [Recovery time objective] and a recovery point objective of [Recovery point objective] for its production service. Each critical system is listed below with its own targets.

System	Recovery time objective	Recovery point objective	Owner
[Production application]	[Recovery time objective]	[Recovery point objective]	[Engineering owner role]
[Production database]	[Recovery time objective]	[Recovery point objective]	[Engineering owner role]

3. Backups

- Backups: All customer data is backed up regularly ([Backup frequency]) to [Backup location], encrypted, and retained for [Backup retention period].

- Restore testing: A backup of the production database is restored to a separate environment at least once a quarter, following section 4.

4. Restore testing

1. Once a quarter, pick the most recent backup of the production database, restore it to a separate, non-production environment, and never over the live database.
2. Verify the data: row counts on key tables match production, a recent record is present, and the application can read it. Record how long the restore took.
3. Record the test in the restore test log with the date, the backup used, the time taken and whether the targets were met, and keep a screenshot or log of the restore. Delete the restored copy when you are done.
4. If the target was missed or data was incomplete, record the issue, fix it, and retest within 30 days.

5. Disaster recovery

- Recovery strategy: Critical systems run across more than one availability zone, and backups are kept in a separate location so the service can be rebuilt if a region is lost.
- Annual test: This plan is exercised at least once a year, by a failover test or a recovery tabletop, and the result is recorded.

6. Recovery procedure

1. Declare the disruption, open an incident record and notify the incident lead under the Incident Response Plan.
2. Assess what is affected and whether recovery objectives are at risk.
3. Decide between waiting for the provider, failing over and restoring from backup, and record who decided and when.
4. Recover the service and verify data integrity before reopening it to customers.
5. Tell customers what happened through [Status page] and direct notice where contracts require it.
6. Hold a review within 5 business days and track every action to completion.

7. People and suppliers

- Every critical system has a named owner and a named backup who can operate it.
- Access to production for recovery does not depend on a single person or a single device.
- For each critical vendor, the Company knows how it would operate if that vendor were unavailable for a day.

8. Roles and responsibilities

Role	Held by	Responsibility
Policy approver	[Policy approver role]	Approves this policy, each new version, and any risk the Company accepts instead of meeting it.
Policy owner	[Security owner role]	Maintains this policy, makes sure the controls in it operate, keeps the evidence, and reviews it at least once a year.
Incident lead	[Engineering owner role]	Runs a recovery, decides on failover or restore, and leads the review afterwards.
All personnel	Everyone in scope	Follow this policy and report a suspected breach of it to the [Security owner role].

9. Evidence and records

The records below show that this policy operates. Each is dated, kept for at least [Evidence retention period], and stored where an auditor can be given it.

Record	What it shows	Where it is kept
Approved policy	This document, signed by the approver, with its version history.	[Documentation system]
Annual recovery test	The failover test or tabletop record, with findings and actions.	[Evidence storage location]
Backup configuration	Screenshot of backup job settings.	[Cloud provider]
Restore test log	Each restore test, the backup used, the time taken and the result.	[Evidence storage location]

10. Exceptions and enforcement

A deviation from this policy needs a written exception approved by the [Security owner role] before it begins. Each exception records the rule not met, the business reason, the compensating control and an expiry date no more than 12 months away. Exceptions are reviewed at each annual review.

A breach of this policy is handled under the Company disciplinary process and may lead to action up to and including termination of employment or contract. A breach that exposes customer data is also handled as a security incident.

11. Review and approval

The [Security owner role] reviews this policy at least once a year and after any significant change to the business, the systems in scope or the risks they face. The [Policy approver role] approves each version. Personnel are told of material changes and acknowledge the current version.

Version	Date	Summary of change	Approved by
[Version]	[Effective date]	First version.	[Policy approver role]

Policy approver

Name:

Signature:

Date:

12. Fields to complete

Replace every bracketed field in this document with your own detail, then delete this section.

Field	What to enter
[Company name]	Your legal company name.
[Effective date]	The date the approver signs this version.
[Version]	Start at 1.0 and increase it each time the document changes.
[Security owner role]	The role that runs the security program day to day, for example Chief Technology Officer.
[Policy approver role]	The officer who approves policies and accepted risks, for example Chief Executive Officer.
[Evidence storage location]	The shared folder or system where evidence is kept.
[Documentation system]	Where policies and procedures are published, for example the company wiki.
[In-scope systems]	The product, cloud accounts and tools inside the audit boundary.
[Cloud provider]	Where production runs, for example AWS, Google Cloud or Azure.
[Recovery time objective]	The longest the service may be down after a disaster, for example 4 hours.

Field	What to enter
[Recovery point objective]	The most data you can afford to lose, for example 24 hours.
[Backup frequency]	For example daily.
[Backup location]	Where backups are kept, separate from the primary data.
[Backup retention period]	For example 30 days.
[Evidence retention period]	How long audit evidence is kept, for example three years.
[Status page]	Where customers see service status, if you publish one.
[Engineering owner role]	The role that owns production systems, for example engineering lead.
[Next review date]	The date this version must be reviewed by, at most 12 months after the effective date.

Source

Source: free template from www.polaralabs.com/templates/business-continuity-plan (CC BY 4.0).