**Disaster Recovery Plan**

# ***Version Control Table***

| Version | Date | Author | Description |
| --- | --- | --- | --- |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| **1.0** |  |  |  |
|  |  |  |  |

| **Date of Next Revision** |  |
| --- | --- |

This policy will be reviewed for continued completeness, relevance, and accuracy within 1 year of being granted “final” status, and at yearly intervals thereafter.

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

# ***Table of Contents***

[**Version Control Table**](#_1t3h5sf) **2**

[**Table of Contents**](#_4d34og8) **3**

[**Purpose**](#_7s6z329mfess) **4**

[**Scope**](#_98gh1c20134h) **4**

[**Disaster Recovery Plan**](#_htj2nywx40qj) **4**

[**Disaster Recovery Team**](#_w74atipusb2a) **4**

[**Critical Systems and Services**](#_g5allkydhzj0) **4**

[**Disaster Recovery Action Plan**](#_81iiqndrfmol) **5**

[**Notification Phase**](#_uxx5r2qmghfm) **5**

[**Recovery Phase**](#_7qthrmi4ht8n) **5**

[**Reconstitution Phase**](#_atx586aeo87r) **5**

[**Forensics Phase**](#_6rbvm7pzwssw) **5**

[**Retrospective Phase**](#_hmv4dmb32xjz) **6**

[**After Disaster Test Phase**](#_6snfqhlw7dm4) **6**

[**Disaster Recovery testing**](#_grmx9find4xd) **6**

[**Change, Review, and Update**](#_w1o88vxspwq8) **6**

[**Disciplinary Action**](#_nubzoem94o3x) **7**

[**Responsibility**](#_hbuyrp1djidk) **7**

[**Related documents**](#_cot3aomf1czt) **7**

# 

# **Purpose**

The purpose of the *[Company]’s* Disaster Recovery Plan is to establish procedures to recover the company’s operations following a disruption resulting from a disaster. The types of disasters contemplated by this plan include natural disasters, political disturbances, manufactured disasters, external human threats, and internal malicious activities. IT Manager maintains this Disaster Recovery Plan.

# **Scope**

This policy includes all resources and processes necessary for service and data recovery and covers all information security aspects of disaster recovery management.

This plan is separate from our Business Continuity Plan, which focuses on how to keep the systems up in the case of an uncommon event.

# **Disaster Recovery Plan**

* The company performs testing of the Disaster Recovery Plan at least annually. The IT Manager is responsible for testing the Disaster Recovery Plan.

## **Disaster Recovery Team**

In case of a disaster, the committee is gathered to discuss the future actions needed for the system recovery. All of the key stakeholders are informed about *[Company]* systems’ current state during the recovery from a disaster.

| **Name** | **Role** | **Responsibility** | **Contact information** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

## **Critical Systems and Services**

The following services and technologies are considered high risks for the business operations, as these systems host application/database servers or are required for the functioning of those systems. These systems, if unavailable, affect the integrity of data and must be restored:

* *[list of critical systems and services]*.

## **Disaster Recovery Action Plan**

### **Notification Phase**

This phase addresses the initial actions taken to detect and assess the damage inflicted by a disruption to the company.

* The first person to report the disaster should notify IT Manager.
* IT Manager notifies team members of the Disaster Recovery Team.
* If *[Company]* is unavailable to customers for more than *[n]* hours, *[Company]* will declare that a disaster has occurred and that the Disaster Recovery Plan has been activated. The other unexpected criteria can start the plan as well.
* Once the Disaster Recovery Plan has been activated, the IT Manager should notify relevant personnel on the general status of the incident.

### **Recovery Phase**

This phase covers the recovery of the application at an alternate site.

* Appropriate personnel assesses the damage done to affected environments, prioritizing critical systems first, and documents observations.
* If possible, makes the backup of the affected environments for forensic purposes without altering them.
* Verifies that backups of critical systems and databases are available.

### **Reconstitution Phase**

This phase consists of activities necessary for restoring the company’s operations to the original operating state (or permanently move operations to the new site).

* Begin replication of the new environment using previously confirmed backups.
* Test the new environment, logging, security, and alerting functionality.
* Verify that systems are appropriately patched and up to date.
* Deploy a new Disaster Recovery environment to production.

### **Forensics Phase**

This phase consists of activities related to finding out the cause of the disaster when it is not immediately apparent.

* Ensure all logs from all systems, applications, and databases involved in the incident have maintained their integrity in the centralized log repository.
* If some logs did not reach the central log repository, ensure that the missing system, database, and application logs are retrieved.
* Analyze all logs.
* Document all significant findings in the timeline.

### **Retrospective Phase**

A retrospective allows all parties to understand what happened in a clear and blame-free manner. A retrospective meeting should occur within 24 hours after the incident has occurred.

* All relevant parties and system owners should be identified and invited to a retrospective meeting.
* Document the retrospective meeting.
* Produce an incident report from the retrospective agenda, timeline, and meeting notes.

### **After Disaster Test Phase**

To analyze the cause of the unanticipated incident, it should be simulated again and documented to better respond in the future.

* Simulate the event. The simulation can be run with people involved or uninvolved in the disaster recovery process.
* Ideas on how to prevent or mitigate a similar event are written down.
* After the simulation, a new and specific playbook should be created.

## **Disaster Recovery testing**

* The plan is tested **annually** and updated based on the results of the testing. IT Manager is responsible for this workflow.

# **Change, Review, and Update**

This policy shall be reviewed once every year unless the owner considers an earlier review necessary to ensure that the policy remains current. Changes to this policy shall be exclusively performed by IT Manager.

# **Disciplinary Action**

Employees who violate this policy may face disciplinary consequences in proportion to their violation. *[Company]’s* management will determine how severe an employee’s offense is and take the appropriate action.

# **Responsibility**

The IT Manager is responsible for ensuring this policy is followed.

# Reference

* *[SOC 2 or ISO 27001 controls]*

# **Related documents**

* Business Continuity Plan
* Incident Response Plan