# Business Continuity Plan

Version 1 - Approved by Youssef Ouyhya

# Contents

1. Objective
2. Scope
3. Plan Objectives
4. Assumptions
5. Disaster Definition
6. Preparation for Disaster Recovery & Business Continuity
7. Instructions for Using the Plan
8. Document Security Classification
9. Non-Compliance
10. Responsibilities
11. Schedule
12. Version history

## 1. Objective

The objective of this business continuity plan is to prepare CNTXT in the event of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible within an acceptable time frame.

## 2. Scope

The scope of this plan is limited to business continuity and disaster recovery of CNTXT's production infrastructure.

## 3. Plan Objectives

- Serves as a guide for the recovery teams of CNTXT.
- References and points to the location of critical data.
- Provides procedures and resources needed to assist in recovery.
- Identifies vendors and customers that must be notified in the event of a disaster.
- Assists in avoiding confusion experienced during a crisis by documenting, testing, and reviewing recovery procedures.

## 4. Assumptions

- Key people (team leaders or alternates) will be available following a disaster.
- A national disaster such as a nuclear war is beyond the scope of this plan.
- This document and all vital records are stored in a secure off-site location and not only survive the disaster but are accessible immediately following the disaster.
- Each support organization will have its own plan consisting of unique recovery procedures, critical resource information, and procedures.

## 5. Disaster Definition

Any loss of utility service (power, water), connectivity (system sites), or catastrophic event (weather, natural disaster, vandalism) that causes an interruption in the service provided by CNTXT operations. The plan identifies vulnerabilities and recommends measures to prevent extended service outages.

## 6. Preparation for Disaster Recovery & Business Continuity

- It is essential that frequent backups are taken, and backups are stored at a redundant location to facilitate restoration in case of a disaster.

- A backup restoration exercise should be performed by the Infra Operations Person with help from the engineering team.
- The Information Security Officer should ensure that a disaster recovery mock drill is conducted by the Engineering team, which will then allow them to invoke this plan effectively. This exercise may be a tabletop exercise based on the availability commitments.
- If required, through the disaster recovery exercise, the Engineering team should evaluate the following:
    - Recovery time objective
    - Recovery point objective

# 7. Instructions for Using the Plan

## 7.1 Invoking the Plan

This plan becomes effective when a disaster occurs.

## 7.2 Disaster Declaration

The Information Security Officer and/or Engineering Head is responsible for declaring a disaster and activating the various recovery teams as outlined in this plan.

In a major disaster situation affecting multiple business units, the decision to declare a disaster will be determined by senior management. The Engineering Team will respond based on the directives specified by senior management.

## 7.3 Plan Review & Maintenance

This document and the disaster recovery mock drill must be reviewed at least once annually.

## 7.4 Notification of Incident/Disaster

- In cases of technical incidents, the Infra Operations Person/On-Call Engineer personnel should contact the Information Security Officer.
- For any operational incident, it is the responsibility of the user/employee to report it as soon as possible through Sprinto App and/or other means like e-mail or telephone, as applicable.
- The Information Security Officer should be notified promptly when any of the following conditions exist:
    - Any server is down for three or more hours.
    - Any problem at any system that would cause the above condition to be present or there is a certain indication that the above condition is about to occur.
- The Information Security Officer should contact the respective CNTXT Business heads and report that a disaster has taken place.

- Once a disaster has been declared, it must follow the incident management procedure and change management procedures while trying to bring back the availability of services.
- Declare a disaster only if the situation is not likely to be resolved within predefined time frames. The person who is authorized to declare a disaster must also have at least one backup person who is also authorized to declare a disaster in the event the primary person is unavailable.
- It is the responsibility of the Information Security Officer to ensure the event of a disaster and the successful recovery are communicated to relevant stakeholders, customers, and regulatory bodies as applicable.

## 8. Document Security Classification

Company Internal (please refer to the Data Classification policy for details).

## 9. Non-Compliance

Compliance with this policy shall be verified through various methods, including but not limited to automated reporting, audits, and feedback to the policy owner. Any staff member found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment or contractual agreement. The disciplinary action shall depend on the extent, intent, and repercussions of the specific violation.

## 10. Responsibilities

The Information Security Officer is responsible for approving and reviewing policy and related procedures. Supporting functions, departments, and staff members shall be responsible for implementing the relevant sections of the policy in their area of operation.

## 11. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization.

---

End of Business Continuity Plan. For version history, please see the next page.

# Version history

| Version | Log | Date |
| --- | --- | --- |
| 1 Current | Policy version approved by Youssef Ouyhya | 26 Oct, 2024 |
| 1 | New Policy version Created | 26 Oct, 2024 |