Centinel Securities Pvt. Ltd.
399, St 58, D-12/2, Islamabad
+92 333 545 9996

CENTINEL SECURITIES (PRIVATE) LIMITED

PAKISTAN STOCK EXCHANGE TRE CERTIFICATE NO. 551

Business Continuity and IT Disaster Recovery Policy

S.No.	Detail	Date
1.	Prepared by Compliance Officer	23 June 2025
2.	Reviewed & Approved by CEO	26 June 2025

Business Continuity and IT Disaster Recovery Policy

1. INTRODUCTION

1.1 This document outlines Centinel Securities (Private) Limited (CSL)'s approach to maintaining operational continuity in the event of a disruption or crisis. It provides a strategic framework for recovering critical systems, IT infrastructure, and communication networks. While this plan presents our preferred response protocols, adjustments may be made in real-time depending on the nature of the emergency to protect systems, personnel, and data.

1.2 The core objective of this plan is to uphold the availability and integrity of information systems and to ensure seamless business continuity.

1.3 In accordance with Regulation 16(10) of the Securities Brokers (Licensing and Operations) Regulations, 2016, issued by the Securities and Exchange Commission of Pakistan (SECP), brokers are required to implement policies that mitigate conflicts of interest and ensure fair dealing with clients. A strong contingency plan forms part of that responsibility.

2. POLICY COMMITMENT

The Board of Directors has adopted the following principles:

2.1 A full review of the Disaster Recovery Plan will be conducted at least once every year.
2.2 Risk assessments will be carried out regularly to evaluate and update recovery requirements.
2.3 The plan shall comprehensively cover essential IT systems, networks, and infrastructure aligned with CSL’s critical functions.
2.4 Simulated testing of the plan will be performed to validate its effectiveness and to familiarize staff with their responsibilities.
2.5 All employees will be trained on the plan and briefed on their specific roles.
2.6 The plan shall be updated continuously to reflect evolving risks, technologies, and business operations.

3. PURPOSE AND OBJECTIVES

The purpose of CSL's Disaster Recovery Plan is to provide a clear and effective roadmap for responding to unexpected events that affect operations. Key goals include:

3.1 Ensuring staff clearly understand their duties during a disaster recovery scenario.
3.2 Confirming that operational policies are consistently applied during implementation.
3.3 Ensuring that contingency solutions are financially prudent and effective.
3.4 Making the recovery framework relevant and usable for employees, service providers, and stakeholders.

4. PLAN STRUCTURE

4.1 Plan Maintenance

Any updates to the Disaster Recovery Plan must follow structured change management procedures. All updates will be tested before adoption and reflected in relevant training materials. These updates will be overseen by the IT team in coordination with the CEO.

4.2 Storage of Documentation

Copies of the recovery plan will be stored securely in designated locations. Each IT team member will receive a hard copy, and a master digital version will be saved on protected systems.

4.3 Preventive Measures

To limit the likelihood and impact of disruptions, CSL has implemented several safeguards:

CENTINEL SECURITIES (PRIVATE) LIMITED ★

- All equipment is housed in secure, access-controlled rooms.
- Access to systems and data is restricted via password protections; only authorized personnel can access servers.
- Uninterruptible Power Supply (UPS) units are deployed to support all critical hardware and networking components.

4.4 Hardware Backup Strategy

Vital business data and system backups are maintained at on-site and remote secure locations and can be restored within 30 minutes in case of failure.

4.5 Risk and Threat Evaluation

A range of threats that may hinder trading or data access have been evaluated based on their likelihood and potential consequences. Key scenarios include:

Disaster Type	**Likelihood (1–5)**	**Impact (1–5)**	**Summary & Mitigation**
Natural Disasters (Flood, Fire, etc.)	1	2	Secure backups stored offsite, recoverable on alternate hardware.
Power Failure	4	2	UPS tested weekly; generators kick in within 10 minutes.
Network Connectivity Loss	3	3	Technical staff on-call for immediate recovery.
Internet Outage	3	3	Auto-switch enabled secondary internet connection.
Network Hardware Failure	3	2	Spare devices kept ready for swap.
Server or Hardware Malfunction	2	1	Redundant systems available.

Rating Scale:

- Likelihood: 1 = Very Low, 5 = Very High
- Impact: 1 = Low, 5 = High

5. TESTING AND SIMULATION

5.1 Conducting regular drills is a vital part of ensuring the recovery plan works as intended. These exercises help evaluate effectiveness, improve team readiness, and highlight any weaknesses.

5.2 Rehearsals help staff gain confidence in executing their roles efficiently during real incidents.

5.3 Following each test, recommendations for improvement may be made. Any changes will be documented, and updates reflected in the official version of the plan.

6. DISASTER RECOVERY KIT

A disaster recovery toolkit will be maintained at the primary office and other designated secure sites. It will contain:

- A printed version of the Disaster Recovery Plan
- A list of all IT team members’ contact details
- Contact information for all employees, including extensions and email addresses

CENTINEL SECURITIES (PRIVATE) LIMITED ★

7. PERIODIC REVIEW

The Contingency and Disaster Recovery Plan will be formally reviewed and updated once a year to ensure its relevance and effectiveness in line with operational changes and emerging threats.

Approved By:

CENTINEL SECURITIES (PRIVATE) LIMITED ★

Chief Executive Officer