PAWAN PARMESHWAR CAPITAL PVT LTD

Regd. Office: 187, Dadiseth Agyari Lane, 4th Floor, Singhania Wadi, Mumbai – 400 002
Head Office: 136-138, ORM Wing B Co-Op Premises Soc. Ltd., Ground Floor, Royal Palm, Goregaon East, Mumbai – 400 065
Tel: 022-22014936 / 4961 3718

Member: NSE Code: 00188 | BSE Code: 0550

Business Continuity Plan and Disaster Recovery Framework

Version 1.0

Document Title	Business Continuity Plan (BCP) and Disaster Recovery (DR) Framework
Version	1.0
Date of Approval	16th October 2025
Effective Date	20th October 2025
Owner	Designated Officer for Cyber Security (DO-CS) with IT and Operations Functions
Approving Authority	Board of Directors of Pawan Parmeshwar Capital Pvt Ltd
Next Review Date	Annually, or earlier upon material change in operations / IT environment / regulatory framework
Replaces	Not applicable — first formal version under SEBI CSCRF

1. Introduction and Purpose

Pawan Parmeshwar Capital Pvt Ltd ("the Company") is a Stock Broker registered with the Securities and Exchange Board of India ("SEBI") and a Trading Member of the National Stock Exchange of India Ltd (NSE Code 00188) and BSE Limited (BSE Code 0550). The Company's ability to execute client orders, settle trades, safeguard client funds and securities, and discharge regulatory reporting obligations is critically dependent on continuous availability of its information systems, premises, connectivity, personnel and Service Providers.

This Business Continuity Plan ("BCP") and Disaster Recovery ("DR") Framework sets out the arrangements that the Company has put in place to:

- Continue critical business operations through a disruption.
- Recover affected systems and operations within defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

- Communicate effectively with clients, regulators, employees and the public during a disruption.
- Restore normal operations following a disruption and incorporate lessons learnt.

The BCP is framed for compliance with the SEBI Cybersecurity and Cyber Resilience Framework dated August 20, 2024 (as clarified by SEBI Circular dated April 30, 2025) ("CSCRF"), the SEBI Master Circular for Stock Brokers SEBI/HO/MIRSD/MIRSD-PoD/P/CIR/2025/90 dated June 17, 2025, the Information Technology Act, 2000, the bye-laws and circulars of NSE and BSE, and the Clearing Corporations.

2. Scope and Applicability

The BCP covers disruptions arising from any of the following categories:

- Cyber Incidents — cyber attack, malware/ransomware, data breach, denial-of-service, compromise of authentication.
- Information Technology Failures — hardware, software, database, network, application, cloud or vendor-system failure.
- Connectivity Failures — Exchange connectivity, internet, telecommunications, leased line.
- Power Failures — including extended grid outage and backup-power failure.
- Premises Disruption — fire, flood, building access denial, civil disturbance affecting the offices.
- Personnel Disruption — pandemic, mass absence, key-person unavailability.
- Vendor / Service Provider Disruption — including critical outsourced functions.
- Natural Calamities — earthquake, cyclone, flooding.
- Public Health Emergencies.
- Any other event materially affecting the Company's ability to operate.

3. Regulatory Framework

- SEBI Cybersecurity and Cyber Resilience Framework dated August 20, 2024 (as clarified April 30, 2025) — BCP/DR is a mandatory component.
- SEBI Master Circular for Stock Brokers SEBI/HO/MIRSD/MIRSD-PoD/P/CIR/2025/90 dated June 17, 2025.
- SEBI (Stock Brokers) Regulations, 1992, including Chapter IVA inserted by SEBI (Stock Brokers) (Amendment) Regulations, 2024 notified on June 27, 2024.
- Information Technology Act, 2000 and rules thereunder.

- CERT-In Directions dated April 28, 2022 (incident reporting timelines apply equally to disruption-causing cyber incidents).
- Bye-laws, Rules, Regulations and Circulars of NSE and BSE.
- Circulars of NSE Clearing Limited and Indian Clearing Corporation Limited.

4. Definitions

5. Governance

5.1 Board Oversight

The Board of Directors is the apex authority for business continuity. The Board:

- Approves this BCP and its periodic revisions.
- Reviews annual BCP/DR testing reports.
- Reviews material disruptions and the Company's response.
- Approves capital expenditure on BCP/DR infrastructure.

5.2 Designated Officer for Cyber Security (DO-CS)

The DO-CS, designated under the Cyber Security and Cyber Resilience Policy v1.0, owns this BCP and reports to the Board on continuity matters. The DO-CS coordinates with the IT function, the Operations function, the Compliance Officer, the senior management and external Service Providers.

5.3 Compliance Officer

The Compliance Officer (Mr. Rajkumar Pandey) coordinates regulatory reporting in respect of disruptions — including notifications to SEBI, NSE, BSE, the Clearing Corporations, CERT-In and the Data Protection Board of India (where applicable) — and integrates this BCP with the broader compliance framework.

6. Critical Business Functions and Recovery Objectives

The Company has identified the following Critical Business Functions, together with indicative RTO and RPO targets. The targets are subject to annual review and to refinement based on testing outcomes.

Critical Business Function	Description	Target RTO	Target RPO
Order Reception and Execution	Receipt of client orders through permitted channels and execution on Exchanges	Within current trading session, ideally within 2 hours	0 — no loss of accepted orders
Trade Capture and Booking	Capture of executed trades in back-office systems and reconciliation with Exchange data	Within current trading day	0 — no loss of executed-trade data
Risk Management	Margin monitoring, exposure limits, MTM, RMS surveillance	Within current trading session, ideally near real-time	Less than 15 minutes
Settlement (Funds and Securities)	Settlement with Clearing Corporation and client pay-in/pay-out	Within the prescribed pay-in / pay-out timeline	0 — no loss of settlement obligations or instructions
Contract Note Generation and Despatch	Generation and email despatch of digital contract notes	Within 24 hours of execution	0 — no loss of executed-trade data
KYC, CKYCR and KRA Operations	Client onboarding, periodic review, KRA / CKYCR upload	Within 1 working day	Less than 24 hours
Books of Accounts and Financial Records	Accounting, ledgers, financial reporting	Within 1 working day	Less than 24 hours
Surveillance and Compliance Monitoring	Trade surveillance, alert review, suspicious-transaction monitoring	Within current trading day	Less than 24 hours
Client Communication	Email, telephony, complaint handling	Within 4 hours	Less than 4 hours

Regulatory Reporting	Reports to SEBI, NSE, BSE, Clearing Corps, FIU-IND, CERT-In	Per prescribed timelines for the specific report	0 for reports based on captured data

RTOs and RPOs above are organisational targets. The Company shall, in line with the CSCRF, document and progressively refine these targets through annual reassessment based on testing outcomes and regulatory expectations.

7. Crisis Management Team and Roles

7.1 Composition

The Crisis Management Team (CMT) shall comprise:

- CMT Lead: The Managing Director / Whole-Time Director (or such other senior officer designated by the Board).
- Designated Officer for Cyber Security (DO-CS) — Deputy CMT Lead.
- Compliance Officer (Mr. Rajkumar Pandey).
- Head of Operations / Settlement.
- Head of Information Technology.
- Head of Dealing Room.
- Head of Human Resources / Administration.
- Such other persons as the CMT Lead may co-opt for the specific incident.

7.2 Roles during a Disruption

- CMT Lead: Overall direction; authority to invoke BCP; authority to communicate with senior regulators, key clients and the public; reports to the Board.
- DO-CS: Coordinates technical response and recovery activities; liaises with vendors and Service Providers; manages technical investigation.
- Compliance Officer: Coordinates regulatory communication (SEBI, NSE, BSE, Clearing Corps, CERT-In, DPB); ensures reporting timelines are met; documents events for subsequent enquiries.
- Head of Operations / Settlement: Manages continuity of trade booking, settlement and client pay-out functions.
- Head of Information Technology: Executes recovery procedures, manages alternate-site activation, supervises restoration.
- Head of Dealing Room: Maintains client order channels, communicates with affected clients.

- Head of HR / Administration: Manages personnel safety, employee communication, premises access and welfare arrangements.

8. BCP Invocation

The BCP shall be invoked by the CMT Lead (or, in his / her absence, by the next-senior member of the CMT present) on occurrence of any event meeting any of the following criteria:

- Loss of access to the Primary premises for an expected duration exceeding 4 hours during business hours.
- Failure of any critical IT system that materially affects a CBF for an expected duration exceeding the RTO for that CBF.
- A material cyber incident invoking the Incident Response Plan.
- Connectivity failure to the Exchanges and/or Clearing Corporations expected to exceed 30 minutes during a trading session.
- Loss of any critical Service Provider's services for an expected duration exceeding their contracted RTO or any agreed equivalent.
- Pandemic or other event affecting personnel availability such that less than the minimum operating headcount can be deployed.
- Any other event that, in the CMT Lead's reasonable judgement, requires invocation.

Invocation shall be recorded in writing with the time, basis, the response actions initiated and the CMT membership convened. Invocation may be partial (limited to specific functions or sites) or full.

9. Continuity Strategies

9.1 Alternate Premises

The Company shall maintain an arrangement for an Alternate Site to which critical operations can be relocated in the event of loss of access to the Primary premises. The company has DR site at 4th Floor Singhania Wadi, 187, DSA Lane, JSS Road, Mumbai 400002. The Alternate Site arrangement may take the form of:

- A secondary office of the Company at a location sufficiently separated from the Primary premises (different fault zone).
- A contracted arrangement with a business-continuity service provider providing seat-readiness.

- Remote working arrangements for personnel with secure connectivity to the Company's systems, subject to the Cyber Security Policy v1.0 and the Mobile Phone Usage Policy v1.0.

The Alternate Site shall be reviewed annually by the DO-CS to confirm readiness.

9.2 Alternate IT Infrastructure (DR Site)

Critical systems shall be configured with a DR site / failover capability appropriate to their criticality:

- Trading-related and time-critical systems: hot-standby / near-real-time replication with the lowest practicable RPO.
- Back-office and supporting systems: warm-standby with periodic data replication.
- Archival and reporting systems: cold-standby with periodic back-up restoration.

The DR site shall be at a location with separate power and connectivity infrastructure from the Primary site. Where these systems are hosted with a Service Provider, the Service Provider shall contractually provide DR arrangements within India in line with the data-localisation principle (cross-reference: Outsourcing Policy v2.0 and Cyber Security Policy v1.0).

9.3 Alternate Connectivity

The Company shall maintain redundant connectivity to the Exchanges (where supported by the Exchange architecture) and shall maintain redundant internet links from different last-mile providers. Mobile connectivity shall be available as a tertiary fall-back.

9.4 Back-up Power

Critical IT infrastructure shall be powered through UPS systems sized to permit graceful shutdown or sustained operation until back-up generator activation. Back-up generators shall be tested periodically (monthly load tests as a minimum).

9.5 Data Back-up and Restoration

Data shall be backed up in accordance with the Cyber Security Policy v1.0 and the data classification:

- Restricted data (KYC, financial, trading, UPSI): back-up at least daily; multiple back-up copies; at least one copy stored off-site / in a different availability zone.
- Confidential data: back-up at least daily.
- Internal and Public data: back-up at the frequency commensurate with the operational need.

Restoration tests shall be conducted periodically, with at least a quarterly sample-restoration test of critical-data back-ups and a full restoration test as part of the annual BCP / DR test.

9.6 Personnel Continuity

Personnel continuity shall be addressed through:

- Cross-training of personnel within each function so that key tasks can be performed by more than one person.
- Documented procedures and standard operating documents enabling cover by trained colleagues.
- Succession planning for key roles (DO-CS, Compliance Officer, CMT Lead, function heads).
- Remote-working capability subject to security controls.

9.7 Service Provider Continuity

Critical Service Providers shall contractually undertake BCP / DR commitments aligned with the Company's RTO / RPO targets, subject to the Outsourcing Policy v2.0 framework. The DO-CS shall maintain a list of critical Service Providers and their stated BCP / DR capabilities, and shall obtain annual evidence of testing.

10. Communication Plan

10.1 Internal Communication

During a disruption, the CMT shall communicate with all personnel through pre-established channels:

- Primary: email and corporate messaging.
- Secondary: SMS and call-tree based on the maintained Personnel Contact List.
- Tertiary: physical messaging at the premises (notice board, supervisor-to-team).

The Personnel Contact List shall be maintained by HR / Administration and reviewed quarterly.

10.2 External Communication — Clients

Clients shall be informed of the disruption to the extent that it affects their ability to transact or receive services. Communication shall be approved by the CMT Lead and may include:

- Email to all clients describing the nature of the disruption (at a level appropriate for public disclosure), the expected duration of impact, the workarounds available and the contact mechanism.
- Notice on the Company's website.

- Telephonic communication with high-impact clients through the Dealing Room.

10.3 External Communication — Regulators

Regulatory communication shall be coordinated by the Compliance Officer, including:

- Notification to NSE and BSE in accordance with their respective bye-laws and circulars.
- Notification to the Clearing Corporations to the extent that settlement is affected.
- Notification to SEBI in accordance with the CSCRF and the SEBI Master Circular for Stock Brokers.
- Notification to CERT-In within 6 hours of identification, where the disruption is caused by a cyber incident falling within the CERT-In Directions dated April 28, 2022.
- Notification to the Data Protection Board of India and to affected Data Principals, where personal data is affected, in accordance with the DPDP Act, 2023 and rules thereunder.

10.4 External Communication — Public / Media

Communication with the public or media shall be authorised by the CMT Lead in consultation with the Board. Spontaneous communication by individual employees with the media is prohibited; queries shall be referred to the designated spokesperson.

11. Resumption and Restoration

Once the underlying cause of the disruption is remediated, the CMT shall:

- Verify that the Primary systems and premises are safe and stable for resumption (data integrity, vulnerability remediation, environmental safety).
- Coordinate a controlled fall-back from the Alternate Site / DR site to the Primary site, with appropriate cut-over windows.
- Reconcile data captured during the disruption between primary and alternate systems.
- Confirm to clients, regulators and personnel that normal operations have resumed.
- Conduct a post-incident review within 30 days of resumption.

12. Post-Incident Review

A post-incident review shall be conducted by the DO-CS in consultation with the CMT, covering:

- Timeline of the disruption from detection to resumption.
- Effectiveness of detection mechanisms and invocation criteria.
- Performance against RTO / RPO targets.
- Adequacy of Alternate Site / DR site arrangements.

- Effectiveness of internal and external communication.
- Performance of Service Providers.
- Root cause and contributory factors.
- Lessons learnt and recommended improvements (process, technology, training, contracts).

The post-incident review report shall be presented to the Board within 60 days of resumption. Recommended improvements shall be tracked through the cyber security risk register (cross-reference: Cyber Security Policy v1.0).

13. BCP Testing

13.1 Annual Testing

The Company shall conduct BCP / DR testing not less than once each financial year. The annual test shall be designed by the DO-CS in consultation with the Compliance Officer and the IT function and shall, over a multi-year cycle, exercise the principal disruption scenarios listed in Section 2.

13.2 Test Types

- Tabletop Exercise: walk-through of a hypothetical disruption with CMT members and key personnel; tests decision-making, escalation, communication.
- Functional Test: actual failover of selected systems or functions to the Alternate Site / DR site, with controlled traffic and data.
- Full BCP Test: invocation of the full BCP with operations conducted from the Alternate Site / DR site for a defined period (typically a half-day or full day), out-of-hours where possible to minimise client impact.

13.3 Test Documentation

Each test shall be documented with: objectives, scope, scenarios, participants, observations, deviations from plan, lessons learnt, and remediation actions. Test reports shall be reviewed by the DO-CS and presented to the Board.

13.4 Recovery Drills with Vendors

Annual or periodic recovery drills shall be conducted with critical Service Providers to validate joint recovery procedures.

14. Records and Retention

The Company shall maintain records of:

- This BCP and its prior versions.
- CBF identification and RTO / RPO target documents.
- Personnel Contact List (current and prior versions).
- Critical Service Provider continuity attestations and test outcomes.
- Alternate Site / DR site arrangements (contracts, attestations, readiness reports).
- Back-up logs and restoration-test outcomes.
- BCP invocation records and incident logs.
- Internal and external communications issued during invocations.
- Regulator notifications and acknowledgements.
- Annual BCP / DR test reports.
- Post-incident review reports.
- Board reporting in respect of BCP matters.

Records shall be retained for not less than 5 (five) years from the date of the relevant event, or such longer period as may be required by reason of pending proceedings, in accordance with the Registers and Records Manual v1.0 and the CSCRF.

15. Reporting and Review

The DO-CS / Compliance Officer shall present to the Board:

- A quarterly BCP status update covering testing outcomes, Service Provider attestations, and Alternate Site / DR site readiness.
- Material disruption events and the response (without waiting for the quarterly cycle).
- Annual BCP / DR test report.
- Post-incident review reports.
- Material communications from SEBI, NSE, BSE, the Clearing Corporations, CERT-In or DPB in respect of BCP matters.

This BCP shall be reviewed annually and amended on any material change in the Company's operations, IT environment, Service Provider arrangements, the CSCRF, or other applicable regulatory framework.

Annexure A — Disruption Response Procedures (Quick Reference)

Scenario	Immediate Steps
Exchange Connectivity Loss	(1) Confirm with Exchange helpdesk. (2) Failover to redundant link. (3) Notify Dealing Room and clients with open orders. (4) Notify Exchange and CMT. (5) If exceeding 30 minutes, invoke BCP.
Primary IT System Failure	(1) IT helpdesk acknowledges and triages. (2) DO-CS assesses. (3) Invoke failover to DR site if RTO at risk. (4) Notify CMT and Compliance. (5) Communicate with affected functions.
Cyber Incident	(1) Invoke Incident Response Plan under Cyber Security Policy. (2) Contain and isolate affected systems. (3) Notify CERT-In within 6 hours if reportable. (4) Notify SEBI / Exchanges. (5) Invoke BCP if disruption material.
Premises Inaccessibility	(1) HR confirms personnel safety. (2) Activate Alternate Site. (3) Enable remote-working access for cleared personnel. (4) Communicate with clients. (5) Coordinate with landlord / authorities for resumption.
Pandemic / Mass Absence	(1) Confirm operating headcount. (2) Activate remote-working. (3) Implement minimum-staffing operations. (4) Cross-deploy trained colleagues. (5) Communicate with clients and regulators.
Critical Vendor Outage	(1) Engage vendor incident management. (2) Activate vendor contingency procedure. (3) Where vendor RTO exceeds Company RTO, escalate. (4) Invoke alternate workarounds where available. (5) Communicate with affected functions.
Power Failure (Primary)	(1) UPS activates. (2) Generator activates. (3) Monitor fuel and load. (4) For extended outage, failover non-critical loads off; consider relocation to Alternate Site.

Annexure B — BCP Test Report Template

Field	Particulars
Test Reference Number	
Test Type (Tabletop / Functional / Full)	
Test Date and Duration	
Scenarios Exercised	
CBFs / Systems Covered	
Participants (Names and Roles)	
RTO Achieved vs Target	
RPO Achieved vs Target	
Deviations / Issues Identified	
Lessons Learnt	
Remediation Actions and Owners	
Target Completion Dates	
Sign-off (DO-CS)	
Sign-off (Compliance Officer)	
Date of Presentation to Board	

Board Approval

This Business Continuity Plan and Disaster Recovery Framework (1.0) has been reviewed and approved by the Board of Directors of Pawan Parmeshwar Capital Pvt Ltd at its meeting held on 16th October 2025.

The Board has also recorded, on the same date, the following:

- The Board approves this Business Continuity Plan and Disaster Recovery Framework as the document required under the SEBI CSCRF dated August 20, 2024 (as clarified April 30, 2025) for the recovery resilience goal, and as the framework for compliance with the SEBI Master Circular for Stock Brokers dated June 17, 2025.
- The Board ratifies the Designated Officer for Cyber Security (DO-CS), as separately appointed by Board resolution, as the owner of this BCP.
- The Board confirms Mr. Rajkumar Pandey as the Compliance Officer responsible for regulatory communication in respect of disruptions (SEBI, NSE, BSE, Clearing Corps, CERT-In, DPB).
- The Board ratifies the Critical Business Functions and indicative RTO / RPO targets set out in Section 6, with the understanding that these targets shall be reviewed annually and refined based on testing outcomes.
- The Board approves the annual BCP / DR testing requirement (Section 13) and directs that the first test under this BCP be conducted within 6 months of the Effective Date.
- The Board directs the DO-CS to publish the initial Personnel Contact List, Critical Service Provider continuity register, and Alternate Site / DR site readiness report within 30 days of the Effective Date.
- Cross-references to related policies (Cyber Security and Cyber Resilience Policy v1.0, Outsourcing Policy v2.0, IT and Data Privacy (DPDP) Policy v1.0, Internal Control Policy v2.0, Risk Management and Surveillance Policy v2.0, Registers and Records Manual v1.0) are noted.

For PAWAN PARMESHWAR CAPITAL PVT. LTD.

Director / Authorised Signatory

PAWAN PARMESHWAR CAPITAL PVT. LTD. MUMBAI

Director / Authorised Signatory
Name: Pawankumar Choudhary
Designation: Director
Place : Mumbai | Date: 16th October 2025