

Muthoot Mercantile Limited

(A Unit of Muthoot Ninan Group)

Regd. Office: 'MUTHOOT FLOORS', 1st Floor, North Block, Opp. W&C Hospital,
Thycaud, Thiruvananthapuram-695 014. ☎ 0471-2774800 CIN: U65921KL1997PLC011260
e-mail: info@muthootenterprises.com website: www.muthootenterprises.com

BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY DRILL POLICY

Business continuity plan and disaster recovery forms significant part of an organisation's overall business continuity management plan which includes policies, standard operating procedures to ensure continuity, resumption and retrieval and recovery of critical business processes. Business continuity plan is to minimise operational, reputational, legal, financial and other material consequences arising from a disaster.

A business continuity plan in the company is designed to ensure uninterrupted operations in gold loan lending, vault safety and data recovery. The core components include collateral security, IT disaster recovery and contingency protocols.

The company has framed board approved BCP&DR policy and its functioning shall be monitored by the Board of the company. **The chief information officer** (CIO) shall be responsible for formulation, review and monitoring of BCP & DR.

CORE COMPONENTS OF BCP

Governance & Oversight:

Managed by the Board of Directors with execution oversight assigned to Chief Information Officer or a dedicated crisis management team

Business Impact Analysis:

Facilitates identification of critical business functions such as loan disbursements, customer collections, transaction processing and regulatory filings

Recovery Objectives:

Defines the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for IT systems and core business processes.

Disaster Recovery Plan:

Strategies to restore data centres and core applications from alternate sites during severe infrastructure failures

Testing and Maintenance:

Mandated Disaster drills **once in a year to validate** the efficiency of people, processes and technology

SCOPE OF COVERAGE

Location: Head office, branches and data centre

Core Systems:

Loan origination, core lending application, payment gateways and accounting database

Resources:

Core personnel, third party vendor platforms and physical infrastructure

Dual Lock Vaults:

Two authorised custodians shall access the vault with OTP from central control room

Surveillance systems:

24x7 CCTV monitoring, motion sensors

ROLE OF BOARD AND EXECUTIVE GOVERNANCE

A) Board of Directors > Annual approval and oversight

B) Crisis Management Team > CFO/COO/AGM/CM's

C) Business Recovery Team > Department Heads are entrusted with execution and operation

EXECUTION OF BUSINESS IMPACT ANALYSIS (BIA)

A) Recovery Time Objective (RTO): The maximum acceptance duration of downtime before service restoration

B) Recovery Point Objective (RPO): The maximum acceptance period of data loss measured in time.

BUSINESS FUNCTIONS AND TARGET RTO & RPO

Tier	Business Functions	Maximum tolerable time	Target RTO	Target RPO
Tier 1	Digital disbursement & payment gateways	2 Hours	1 Hour	Near Zero
Tier 1	Core lending database & customer ledgers	4 Hours	2 Hours	< 15 Minutes
Tier 2	Customer service support channels	24 Hours	8 Hours	4 Hours
Tier 3	Regulatory reporting & Financial accounting	72 Hours	24 Hours	24 Hours

DISASTER RECOVERY STRATEGY

A) DATA ARCHITECTURE AND BACKUP REDUNDANCY

1) Primary Infrastructure:

Cloud based or on-premise primary data centre hosting live transactional financial systems.

2) Secondary Site:

Geographically / location separated disaster recovery site configured in active-passive setup

3) Data Replication:

Synchronous replication for Tier 1 transaction logs and asynchronous hourly replication for peripheral data

B) ALTERNATE OPERATIONAL WORKSPACES

1) Remote access:

Pre-configured virtual private network (VPN) profiles for critical staff to execute operations from remote locations.

2) Physical worksite:

Reciprocal arrangement or leased sites at third party business continuity centre for essential personnel.

ACTIVATION OF INCIDENT RESPONSE AND COMMUNICATION

A) INCIDENT DECLARATION SEQUENCE

1) Detection:

IT Monitoring systems or operational teams identify an infrastructure outage or localized disaster

2) Escalation:

Incident manager at IT cell conducts a rapid assessment and briefs the **crisis management team**

3) Declaration:

The crisis management team officially declares a disaster state if recovery cannot occur within RTO boundaries

B) INTERNAL & EXTERNAL COMMUNICATION CHANNELS

1) Employee notification:

SMS alerts, corporate e-mails and dedicated messaging channels.

2) Regulatory reporting:

Official notification despatched to the regulators within the mandated timeline post disaster declaration.

3) Customer communication:

Public notices on the company website to preserve institutions image/trust.

CONDUCT POLICY MAINTENANCE & TESTING

A) MANDATORY DRILLS & TESTING FREQUENCY:

1) Table top exercise:

Bi-annual structured discussion sessions to review team roles and scenario based decisions

2) Live DR drill:

Full live failover switch to the secondary DR site at least once in a year during low traffic period

B) AUDIT AND CONTINUOUS POLICY IMPROVEMENT:

1) Internal Audit:

Annual independent review of BCP compliance, data backup validity, and actual RTO performance during drills.

2) Policy revisions:

Immediate updates following material changes to technology architecture, corporate structure or financial regulations

The Business Continuity Plan and Disaster Recovery Policy is approved for implementation on 18th April 2026.

For Muthoot Mercantile Limited

S/d

Mathew Mathaininan

Chairman & Whole-time Director

DIN: 00063078