JMJ FINTECH LIMITED
(Formerly Known as Meenakshi Enterprises Limited)

BUSINESS CONTINUITY PLANNING (BCP) AND DISASTER MANAGEMENT POLICY

Approved in the board Meeting dated (08/02/2023)

BUSINESS CONTINUITY PLANNING (BCP) AND DISASTER MANAGEMENT

As per the RBI/DNBS/2016-17/53 (Master Direction DNBS. PPD.No.04/66.15.001/2016-17) dated June 8, 2017 issued by Reserve Bank of India, provides guidelines on IT Framework for the NBFC sector, requiring to put in place a Business Continuity Planning (BCP) policy for the NBFCs which will help to minimize operational, financial, legal, reputational and other material consequences.

Business Continuity Planning for IT Services

There shall be a BCP defined for the critical business processes in *JMJ FINTECH LIMITED* (herein referred as "the Company") in terms of the availability of IT assets to keep critical business/process continue even in case of disaster. A business continuity planning process shall be implemented to minimize the impact on the Organization and recover from the loss of information assets to an acceptable level. Business Continuity plan shall be developed and implemented to ensure the timely resumption of critical functions. The plan shall be periodically tested and kept updated.

Objective:

- Implement a process of risk and business impact analysis of major failures or disasters resulting in loss of resources supporting the business processes
- Mitigate the risk of interruptions to business activities from the effects of such major failures or disasters
- Develop a continuity plan and implement the controls to mitigate the impact of disaster and timely resumption of business activities to minimize losses.
- To verify the established and implemented information security continuity.
- To ensure availability of information processing facilities in case of any disaster.

BUSINESS CONTINUITY PLANNING (BCP) POLICY

Policy Goal

The goal for setting up a Business Continuity Planning System (BCPS) at is to put in place appropriate measures that can ensure continuity of IT critical business processes and IT Services & Operations with minimal interruption in the event of a Significant Business Disruption.

IT BCM Policy Statement

A business continuity management process shall be implemented to minimize the impact on the Organization and recover from the loss of information assets to an acceptable level. Business Continuity plan shall be developed and implemented to ensure the timely resumption of critical functions. The plan shall be periodically tested and kept updated.

IT Business Impact Analysis & Risk Assessment

The IT Business Impact Analysis is in line with the Company's BCP Policy.

- Before designing IT business continuity strategy, events (data unavailable, electrical/ power failure, equipment malfunction, fire, software error, strike etc.) which can cause interruptions to the IT processes shall be identified.
- The risks associated with identified events in terms of their likelihood of occurrence and impact shall be calculated and the critical IT business processes be prioritized.
- A detailed Risk Assessment shall be carried out on the basis of IT Business Impact Assessment.
- Risks, controls and Residual Risks shall be identified.
- IT Business continuity strategies shall be developed to determine the overall approach to IT business continuity depending on the results of the IT business impact analysis.

IT Business Continuity Strategy

- Key assumptions regarding the type of incidents, disaster probability, available resources and recovery timeframes shall be documented in IT BCP Policy.
- The IT BCP shall comprise of IT Business Continuity Plans and IT Disaster Recovery Plans.
- An IT business continuity strategy supported by IT business continuity plans shall be formulated and documented in line with the Company's Business Continuity Management Policy.
- The key IT processes shall be mapped with information processing systems within the Company's IT Department and appropriate controls shall be chosen.

IT Business Continuity Planning Policy

- Plans shall be developed to maintain and restore critical IT operations and services in the required time scales following interruption or failure.
- The IT BCP process shall consider the following but not limited to:
- Identification and agreement of all responsibilities and emergency procedures;
- Implementation of emergency procedures to allow recovery and restoration in required time-scales, Particular attention needs to be given to the assessment of external business dependencies and the contracts in place;
- Documentation of procedures and processes;
- Appropriate education of staff in the agreed emergency procedures and processes including crisis management; and
- Testing and updating of the plans.
- The planning process shall focus on the required IT objectives, e.g. restoring critical IT services in an acceptable amount of time. The IT services and resources that enable this to occur shall be considered, including staffing, non-information processing resources, as well as fall back arrangements for information processing facilities.

IT BCP Organization

The IT BCP Organization is in line with Business continuity plan.

- Depending on the size and volume of the Company Chief Information Officer (CIO), IT Department, IT BCP coordinators and IT recovery teams shall be identified.
- CIO of the Company will be responsible for formulation, review and monitoring of BCP to ensure continued effectiveness including identifying critical business verticals, locations and shared resources to prepare a detailed business impact analysis.

Redundancies

- Availability of Information processing facilities shall be ensured.
- Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.
- The Company's CIO/ IT Department shall identify availability of IT systems for Business Operations. Where the availability cannot be guaranteed using the existing systems architecture, redundant components or architectures shall be considered.
- Where applicable, redundant IT systems shall be tested to ensure the failover from one component to another component works as intended.

IT BC Plan Testing & Exercises

The CIO shall develop a test plan designed to test the selected element(s) against explicit test objectives and success criteria. These shall include but not limited to:

- Table-top testing of various scenarios (discussing the IT business continuity and IT DR recovery arrangements using example interruptions);
- Simulations (particularly for training IT people in their post-incident/crisis management roles);
- Technical recovery testing (ensuring that Company's IT systems can be restored effectively);
- Testing recovery at an alternate site (running IT processes in parallel with IT recovery operations away from the main site);
- Complete rehearsals (testing that the IT department, personnel, equipment, facilities and processes can cope with interruptions).

Maintaining & Updating IT BCP Policy

- In coordination CIO, this policy will be reviewed by the Company on an annual basis or as mandated by a sudden change in the business, legal, regulatory or other compliance requirements.
- IT Business Continuity plans shall be maintained at regular intervals and updated to ensure their continuing effectiveness.

Enforcement

- Compliance with this IT Business Continuity Policy is Mandatory.
- All Department Heads must ensure continuous compliance monitoring within their functions. Compliance with this IT Business Continuity Policy will be a matter for periodic review by the CIO of the Company.
- Violations of the IT BCP Policy may result in corrective action by management.

IT BCP Objectives

The aim of BCP framework is to inform and drive continual, effective, cross-functional, continuity planning through holistic, integrated risk management practice. Key objectives of the framework are as follow:

- To develop IT Department Business Continuity capability in line with industry best practices and international standard like ISO 22301:2012.
- To develop workforce capabilities and competencies through plans, skill trainings and role rehearsals, and adequate provision of technical equipment and committed resources
- To recover and protect the critical IT activities supporting business operations thereby reducing any subsequent financial impact to the organization.
- To provide a consistently clear view of the approach to be taken regarding Incident Response & Management and IT Business Continuity within the Company.
- To protect the organization’s brand and minimize any adverse impact to it.
- To identify and manage IT Business Continuity and Information Security related risks
- To ensure that Company meets legal, regulatory and contractual obligations and protect its reputation.
- Establish necessary roles and responsibilities for successful planning, implementation, operation, monitoring and review of IT BCP on an on-going basis.
- Ensure IT BCP Plans and procedures are exercised at regular intervals and are maintained up to date.
- Promote IT BCP awareness through communication of approved policies, standards, plans, procedures, guidelines
- Provide specific IT BCP training to department heads and staffs to enable them to respond to any major incident in a planned manner.

FOR JMJ FINTECH LIMITED

Sd/-

Managing Director