N.B.I. INDUSTRIAL FINANCE COMPANY LIMITED

BUSINESS CONTINUITY PLAN

(Plan approved by the Board of Directors of the Company at their meeting held on 16.05.2024)

1. Introduction:

Interruptions to business functions can result from major natural disasters such as earthquakes, floods, and fires, or from man-made disasters such as terrorist attacks, riots or war. The most frequent disruptions are less sensational—equipment failures, theft.

Business Continuity Plan (BCP Plan), also known as Contingency Planning, defines the process of identification of the applications, customers (internal & external) and locations that a business plans to keep functioning in the occurrence of such disruptive events, as well the failover processes & the length of time for such support. This encompasses hardware, software, facilities, personnel, communication links and applications.

Company and its associates are mainly and majorly involved in investing business activities with insignificant and negligible / Nil lending business activity and is categorized as Non- Deposit taking Middle layer NBFC-ICC.

Significant and substantial business assets are maintained in digital form (Shares in demat form) / with Mutual Fund which are not vulnerable and material / Man Made disasters and therefore does not impact business continuity. As loaning activity is negligible, customer data are very few and are in physical form. Business transactions are maintained on off the shelf, ready available, plug and play, uncustomized software, which is backed up and for which maintenance support available easily. With this background, the Company had formulated its BCP Plan.

This document serves the purpose of codification of a formal policy of existing practices followed by the Company and is meant for continuing guidance.

BCP plan is intended to enable a quick and smooth restoration of operations after a disruptive event. The BCP plan also defines actions to be taken before, during, and after a disaster.

This Plan comes into effect on and from 16.05.2024.

2. Purpose:

The plan has been developed to allow for Continuity of Business operations at a minimum level in the event of an emergency.

3. Scope of Plan:

This plan applies to all employees, partners, stakeholders and parties associated to the Company.

4. Objective of Business Continuity Plan:

- Protect personnel, assets and information resources from further injury and/ or damage
- Minimize economic losses resulting from disruptions to business functions
- Provide a plan of action to facilitate an orderly recovery of critical business functions

- Identify key individuals who will manage the process of recovering and restoring the business after a disruption
- Specify the critical business activities that must continue after a disruption
- Minimize damage and loss
- Resume critical functions at an alternate location
- Return to normal operations when possible.

5. Key features of the Plan:

The components of Company's Plan are as follows:

- **Strategy**: Objects that are related to the strategies used by the Company to complete day-to day activities while ensuring continuous operations.
- **Organization**: Objects that are related to the structure, skills, communications and responsibilities of its employees.
- **Applications and data**: Objects that are related to the software necessary to enable business operations, as well as the method to provide high availability that is used to implement that software.
- **Processes**: Objects that are related to the critical business process necessary to run the business, as well as the IT processes used to ensure smooth operations.
- **Technology**: Objects that are related to the systems, network and industry-specific technology necessary to enable continuous operations and backups for applications and data.
- **Facilities**: Objects that are related to providing a disaster recovery site if the primary site is destroyed.

6. Procedure:

This is a disaster recovery plan for N.B.I. Industrial Finance Co. Ltd. (NBI). The information present in this plan guides NBI's operation & Data management in the event that a disaster destroys all or part of the facilities. The primary focus of this BCP is to respond to a disaster that destroys or severely cripples NBI's operation & Data computer systems. The intent is to restore operations as quickly as possible with the latest and most up-to-date data available.

Disaster recovery plans are developed to span the recovery of data, systems, links and also include worst case scenarios such as:

- Loss of access to facility
- Loss of access to information resources
- Loss of key personnel who are responsible for performing critical functions

7. Personnel:

Immediately following the disaster, a planned sequence of events begins. Key personnel are notified to implement the plan.

8. Salvage Operations at Disaster Site:

Early efforts are targeted at protecting and preserving the computer equipment. In particular, any storage media are identified and either protected from the elements or removed to a clean, dry environment away from the disaster site.

9. Designate Recovery Site / Alternate site / Backup site:

As per the IT infrastructure of the Company commensurate with its size and operations regular backups shall be taken in other external memories/connected devices. Company follows 3 backup policy. Earlier baked up data are deleted.

Data back up is taken, in full, twice a week, in E Drive of server and a copy is stored in another machine. Data back up is also taken on external hard disk on monthly basis.

10. Purchase New Equipment:

Hardware / Equipments deployed are not high end. The recovery process relies upon vendors to quickly provide replacements for the computer resources that cannot be salvaged.

11. Begin Reassembly at Recovery Site:

Salvaged and new components are reassembled at the recovery site. If vendors cannot provide a certain piece of equipment on a timely basis, then recovery personnel can make Last-minute substitutions. After the equipment reassembly phase is complete, the work turns to concentrate on the data recovery procedures.

12. Restore Data from Backups:

Data can be restored from the backups available within office premises and outside as well in the external drives.

13. Prevention:

As important as having a disaster recovery plan is, taking measures to prevent a disaster or to mitigate its effects beforehand is even more important. This portion of the plan reviews the various threats that can lead to a disaster and steps Company to take to minimize the risk. The threats covered here are both natural and human-created:

- **Fire & Flood**
- **Earthquake**
- **Computer Crime**

Fire & Flood- The threat of fire in office premises is real and poses a high risk. The office premises are filled with electrical devices and connections that could overheat or short out and cause a fire.

The office is equipped with a fire alarm system. Ceiling mounted fire extinguishers are placed in visible and important locations throughout the building.

The threat of flood is very low considering past history. Remote access to the application is provided for emergent business operation.

Earthquake - The threat of an earthquake is medium to low but should not be ignored. An earthquake has the potential for being the most disruptive for this disaster recovery plan. Restoration of computing and networking facilities following a bad earthquake could be very difficult and require an extended period of time due to the need to do large scale building repairs.

Computer Crime- Computer crime is becoming more of a threat as systems become more complex and access is more highly distributed. With the new networking technologies, more potential for improper access is present than ever before. Computer crime usually does not affect hardware in a destructive manner. It may be more insidious, and may often come from within.

To avoid Computer and cybercrimes, genuine antivirus are used to protect private and financial information online.

All systems are protected by password to protect against unauthorized entry. All users are required to change their data application password on regular basis.

Training - As and when required and if needed a training programme might be scheduled for the employees with respect to above.

14. Execution:

The Company through its Board of Director's direct supervision ensures the implementation of the policy at the operational level and may hire the services of subject matter experts for effective management and risk control.

15. Security Awareness:

• Employee awareness is boosted through one to one interaction considering limited employee base.

• Unless expressly authorized to do so, user is prohibited from sending, transmitting, or otherwise distributing proprietary information, data, or other confidential information.

16. Policy Review - The Plan shall be reviewed by the Board subject to guidelines issued by RBI and to make amendments if considered necessary.

17. Adoption - This Plan and any changes made during the reviews shall be adopted by the Board of Directors.