DHUNSERI INVESTMENTS LIMITED

BUSINESS CONTINUITY PLAN

1. Introduction:

Business operations may be disrupted due to unforeseen circumstances, including natural disasters such as earthquakes, floods, fires and other calamities, as well as man-made incidents such as terrorist activities, riots, sabotage, cyberattacks, equipment failures, theft or technical malfunctions.

A Business Continuity Plan (BCP), also referred to as a Contingency Plan, establishes a structured framework for identifying critical business functions, operational dependencies, information systems, personnel and resources necessary to ensure continuity of business operations during unforeseen disruptions.

The Business Continuity Plan of Dhunseri Investments Limited (hereinafter referred to as the "Company") is designed to facilitate the timely restoration of critical business operations, minimise operational and financial losses, safeguard information assets and ensure the continuity of essential services in the event of a disruption.

The Plan outlines the preventive, responsive and recovery measures to be undertaken before, during and after a disruptive event to enable the Company to resume its normal business operations in an orderly and efficient manner.

2. Purpose:

The purpose of this Business Continuity Plan is to establish an effective mechanism for ensuring the continuity of the Company's essential business operations during emergencies, disasters or other unforeseen disruptions.

The Plan aims to minimise interruptions to business activities, protect the Company's assets and information resources, and facilitate the timely restoration of critical operations with minimum operational, financial and reputational impact.

3. Scope of Plan:

This Business Continuity Plan shall be applicable to all employees, directors, officers, key managerial personnel and other stakeholders associated with the Company, including third-party service providers, wherever relevant.

The Plan shall cover the Company's critical business functions, information technology infrastructure, operational processes, data management systems, communication facilities and other resources essential for the uninterrupted conduct of its business activities.

4. Objective of Business Continuity Plan:

The primary objectives of the Business Continuity Plan are as follows:

- To safeguard the lives, safety and well-being of employees and other personnel during emergencies or disruptive events.

- To protect the Company's physical assets, financial resources, information systems and confidential data against potential damage, loss or unauthorised access.
- To minimise financial, operational and reputational losses arising from interruptions to business operations.
- To mitigate potential losses relating to the Company's investments arising from disruptions affecting its operations or those of its investee companies.
- To establish a systematic and coordinated approach for the recovery and restoration of critical business functions.
- To identify and designate key personnel responsible for managing business continuity and disaster recovery activities.
- To identify essential business activities that must continue or be restored on priority during a disruption.
- To provide suitable alternative arrangements for carrying out critical business operations where normal facilities become unavailable.
- To ensure the availability, integrity and confidentiality of critical business information and records.
- To facilitate the timely restoration of normal business operations following the resolution of the disruptive event.

5. Key Components of the Business Continuity Plan:

The Business Continuity Plan of the Company shall comprise the following key components:

- ***Business Continuity Strategy:*** The Company shall establish appropriate strategies and procedures to ensure the continuity of its essential business activities during disruptions. Such strategies shall be commensurate with the nature, scale and complexity of the Company's operations.
- ***Organizational Structure and Responsibilities:*** The Plan shall identify the roles, responsibilities, reporting mechanisms and communication procedures applicable to employees and designated personnel responsible for implementing business continuity and recovery measures.
- ***Applications and Data Management*****:** 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.
- ***Business Processes:*** The Company shall identify critical business processes and establish appropriate procedures to facilitate their continuation or timely restoration during operational disruptions.
- ***Technology:*** The Company shall maintain appropriate information technology systems, communication networks, data backup arrangements and other technological resources

necessary to support business continuity and disaster recovery.

- ***Facilities and Alternative Arrangements:*** Where necessary and feasible, the Company shall make suitable alternative arrangements for carrying out essential business activities in circumstances where its primary office premises or operational facilities become inaccessible or unusable.

6. Procedure:

The Business Continuity Plan shall serve as a guiding framework for the Company's response to disasters or unforeseen events that may adversely affect its operational facilities, information systems, business records or critical functions.

The primary objective of the disaster recovery procedures shall be to restore essential business operations as expeditiously as practicable while ensuring the security, integrity and availability of critical business information.

The Company shall adopt appropriate recovery measures in circumstances including, but not limited to, the following:

- Loss of access to office premises or other operational facilities.
- Loss of access to critical information systems, applications or business records.
- Failure or damage to computer systems, hardware, software or communication networks.
- Unavailability of key personnel responsible for performing essential business functions.
- Cybersecurity incidents, unauthorised access, data breaches or other information security threats.
- Disruptions involving critical third-party service providers or other operational dependencies.

Upon identification of a significant disruption, the designated personnel shall assess its nature and severity and initiate appropriate recovery measures in accordance with this Plan.

7. Personnel:

In the event of a disaster or significant operational disruption, the designated personnel shall be responsible for initiating and coordinating the implementation of the Business Continuity Plan.

The Company shall maintain updated contact details of relevant employees, management personnel and other essential service providers to facilitate timely communication during emergencies.

8. Salvage Operations at Disaster Site:

Following the occurrence of a disaster, the Company shall undertake appropriate measures to safeguard and recover its physical assets, information technology equipment, records and other essential resources, subject to the safety of personnel and the prevailing circumstances.

Priority shall be given to identifying and securing critical computer systems, storage devices, electronic records and other information resources that may be vulnerable to damage or loss.

Where feasible, storage media and other recoverable equipment shall be relocated to a safe and secure environment to prevent further deterioration or unauthorised access.

All salvage and recovery activities shall be undertaken in a controlled manner, ensuring that the safety of personnel remains the foremost consideration.

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

Considering the nature, size and complexity of its operations and existing information technology infrastructure, the Company shall maintain appropriate arrangements for safeguarding critical business data and facilitating the recovery of essential operations.

Regular backups of important electronic records, applications and other business information shall be maintained through suitable external storage devices or other secure backup mechanisms.

In circumstances where the primary office premises become inaccessible or unsuitable for operations, the Company may implement alternative working arrangements or identify a suitable recovery location, depending upon operational requirements and available resources.

The Company shall endeavour to ensure that such arrangements facilitate the continuation or timely restoration of critical business activities.

10. Purchase New Equipment:

In the event of damage, destruction or failure of critical information technology equipment or other operational resources, the Company shall initiate appropriate measures for their repair, replacement or procurement.

11. Begin Reassembly at Recovery Site:

Upon identification of a suitable recovery location or restoration of the existing premises, the Company shall initiate the reassembly and reinstallation of salvaged or newly procured equipment and other necessary operational resources.

12. Restore Data from Backups:

The Company shall maintain appropriate data backup arrangements to facilitate the recovery of critical business information in the event of system failure, data loss or other operational disruptions.

Backups of essential electronic records and business data shall be undertaken at appropriate

intervals, considering the nature and importance of the information.

Such backups may be maintained through secure external storage devices, designated backup systems or other suitable mechanisms, including storage arrangements outside the primary office premises, wherever feasible.

In the event of data loss or system failure, the designated personnel shall initiate the restoration of information from the latest available reliable backup.

The Company shall take reasonable measures to verify the completeness, accuracy and integrity of restored data before resuming normal business operations.

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, where our vulnerabilities are, and steps we should take to minimize our risk. The threats covered here are both natural and human-created:

- **Fire**
- **Earthquake**
- **Computer Crime**
- **Terrorist Actions and Sabotage.**

Fire - 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 offices are equipped with a fire alarm system. Ceiling mounted fire extinguishers are placed in visible and important locations throughout the building.

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 firewalls and antivirus are used to protect private and financial information online.

All systems have security products installed to protect against unauthorized entry. All systems are protected by passwords. All users are required to change their passwords on a regular basis.

All systems should log invalid attempts to access data, and the system administrator reviews these logs on a regular basis.

Terrorist Actions and Sabotage - Terroristic action and sabotage is potential risk in big cities. To prevent such occurrence Pilani's office building has system in place whereby each person will be permitted entry on verification of personal details and due care is taken to provide adequate security. CCTV cameras is been installed, which gets monitored regularly by the building authorities.

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

14. Security Awareness:

Employee awareness is boosted through security screensaver on PCs along with regular e-mail communication to users.

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

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

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