BUSINESS CONTINUITY PLAN (BCP)

1. PURPOSE

The Reserve Bank of India ("RBI") issued the Reserve Bank of India (Non-Banking Financial Companies – Cybersecurity, Technology, Risk, Resilience and Assurance Framework) Directions, 2026, dated 31st July 2026 (hereinafter referred to as *"the RBI Directions 2026*"), which prescribe guidelines for the technology, cybersecurity and resilience framework for the NBFC sector.

This Business Continuity Plan ("BCP") sets out a proportionate framework to enable HB Stockholdings Limited ("the Company"), a listed, non-deposit-taking and investment-focused NBFC, to maintain operational resilience and minimize disruptions arising from unforeseen events.

2. SCOPE

This BCP applies to all functions and operations of the Company. Further, it aligns with the company's Board approved IT/IS policy to ensure clarity, consistency and comprehensive protection of the Company's business operations.

3. REGULATORY FRAMEWORK

This BCP has been framed with reference to the applicable regulatory requirements and guidelines issued by the Reserve Bank of India (RBI) and the Securities and Exchange Board of India (SEBI), including the following, as applicable and as amended from time to time:

- RBI Master Direction – Reserve Bank of India (Non-Banking Financial Company – Scale Based Regulation) Directions, 2025;
- Reserve Bank of India (Non-Banking Financial Companies – Cybersecurity, Technology, Risk, Resilience and Assurance Framework) Directions, 2026;
- SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 (SEBI LODR Regulations);
- SEBI (Prohibition of Insider Trading) Regulations, 2015, in respect of handling of unpublished price sensitive information (UPSI) during a disruption;

4. OBJECTIVES

The objectives of Company's BCP are as follows:

i. identify, manage and mitigate risks that may affect business continuity.

ii. Assign knowledgeable personnel and sufficient financial resources for effective BCP implementation.
iii. Ensure annual review of BCP.
iv. Evaluate contingency planning for critical outsourced operations.
v. Prioritise recovery of critical business activities within predetermined timeframes.

5. GOVERNANCE AND RESPONSIBILITIES

- **Board of Directors:** Approves the BCP, review it at least annually and ensures adequate resources.
- **Risk Management Committee:** Oversees implementation and reviews incidents and drill reports.
- **All Employees:** Understand their respective roles and responsibilities under the BCP and comply with the prescribed procedures and instructions during a disruption.

6. BUSINESS IMPACT ANALYSIS AND RECOVERY OBJECTIVES

The Company conducts a Business Impact Analysis ("BIA") at least annually to identify critical business activities and processes essential to its operations. The BIA outlines a hierarchy of essential services and processes, ensuring that they are continued or recovered within predefined timeframes in the event of disruptions.

Key activities prioritized for recovery:

- Investment operations, including trade execution, settlement, custody and portfolio monitoring;
- Critical financial services, loan disbursements and collections.
- IT infrastructure, communication and email systems:
- Regulatory reporting: Submission of required financial and regulatory filings.

7. ACTION PLANS FOR RECOVERY:

For each critical business activity, a recovery plan is developed, including:

- Responsible teams: Designated teams shall be identified for each critical business activity and shall be responsible for executing the recovery measures within the prescribed timeframes.
- Predefined timeframes for recovery: Each critical activity is assigned a Recovery Time Objective (RTO) to ensure continuity or recovery within predetermined periods *(e.g., 2 hours, 6 hours, 24 hours, as applicable)*.
- Detailed action steps: Clear steps are outlined for how teams will continue or recover prioritized activities, such as rerouting workflows, activating backup systems, and engaging external partners.

8. INFORMATION SECURITY AND CYBERSECURITY:

The Company ensures robust information security and cybersecurity measures to safeguard its information systems and business operations, including:

- Implementing a maker-checker system to prevent errors or misuse.
- Safeguarding sensitive information through end-to-end encryption for mobile financial services.
- Using digital signatures for authentication of electronic documents and fund transfers.
- Establishing data access controls to restrict unauthorized access to critical information systems.

9. DATA BACK-UP AND RESTORATION:

The Company conducts regular and secure backups of all essential business data, with appropriate onsite and offsite storage arrangements, as applicable. The backup strategy shall include:

- Daily, weekly, and monthly backups to ensure data protection.
- Periodic testing of backup systems through data restoration drills to confirm backup effectiveness.

10. COMMUNICATION AND DISCLOSURE

- Cyber incidents shall be reported to RBI within the applicable prescribed timelines and in accordance with the relevant regulatory requirements.
- Events material to the Company shall be disclosed to the stock exchanges as required under SEBI LODR Regulations.

11. UPDATE AND REVIEW

The Company shall update its BCP whenever significant changes occur, n its business operations, organizational structure. Function-specific plans are also reviewed at least annually to incorporate any operational updates or new regulatory requirements.

12. BOARD OVERSIGHT AND REVIEW:

The Board of Directors plays a critical role in the oversight of the BCP, conducting annual reviews and approving necessary updates. The Board ensures that the Company's business continuity strategies remain effective, relevant, and aligned with regulatory requirements.

13.APPROVAL

This BCP is approved by the Board of Directors and takes effect from the date of approval. Any material amendment to the BCP shall require the approval of the Board of Directors.