INFORMATION TECHNOLOGY / INFORMATION SECURITY (IT/IS) POLICY

HB STOCKHOLDINGS LIMITED

1. PREAMBLE

The Reserve Bank of India ("RBI"), vide 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*"), has prescribed requirements relating to information technology, information security, cybersecurity, technology risk management, operational resilience and business continuity for Non-Banking Financial Companies ("NBFCs").

HB Stockholdings Limited ("the Company") is a non-deposit-taking NBFC classified in the Base Layer, with an asset size below Rs. 500 Crore. This Policy sets out the principles, standards, controls, roles and responsibilities governing the Company's IT systems and information assets, including information security, cybersecurity, access management, data protection, IT risk management, third-party technology arrangements, incident management, data backup and recovery, and business continuity and disaster recovery.

The Policy shall be implemented in accordance with applicable statutory and regulatory requirements, including the RBI Directions, 2026, and in a manner proportionate to the nature, scale, complexity and risk profile of the Company's business, IT infrastructure and technology-related activities.

2. OBJECTIVES

The objectives of this Policy are:

I. To establish a framework for the secure, efficient and reliable use of the Company's IT systems and information assets.

II. To protect the confidentiality, integrity, authenticity and availability of the Company's electronic records and business data.

III. To establish physical and logical access controls that prevent unauthorised access to IT systems and data.

IV. To define user roles, responsibilities and access privileges.

V. To implement password management, authentication and cybersecurity controls.

VI. To establish maker-checker controls, wherever appropriate, to minimise errors, misuse and unauthorised transactions;

VII. To ensure the secure maintenance, storage, backup and recovery of electronic records and business data;

VIII. To identify, assess, monitor and mitigate IT-related risks, including cybersecurity threats and vulnerabilities;

IX. To ensure that IT systems adequately support financial reporting, management information systems and regulatory reporting;

X. To establish controls over third-party IT service providers and outsourced technology arrangements;

XI. To provide for the identification, reporting, investigation and resolution of cybersecurity incidents;

XII. To establish an effective Business Continuity Plan ("BCP") framework to minimise disruption to business operations.

XIII. To ensure periodic review of the effectiveness of IT controls and compliance with applicable statutory and regulatory requirements.

3. SCOPE AND APPLICABILITY

3.1 This Policy applies to the Company and its directors, key managerial personnel, employees, consultants, contractual personnel and other authorised users who access or use the Company's IT systems or information assets. All such persons shall comply with this Policy and with the information security practices and procedures prescribed by the Company.

3.2 The Policy covers, as applicable:

a. computers, laptops, servers and other IT equipment;
b. accounting, financial and business applications;
c. electronic records, business documents and regulatory reporting data;
d. official email accounts and electronic communication systems;
e. Digital Signature Certificates (DSCs);
f. data storage and technology services;
g. backup and recovery arrangements;
h. IT service providers, software vendors and other relevant third parties; and
i. banking and financial transaction systems used by the Company.

The Policy has been formulated with reference to the applicable provisions of the RBI Directions, 2026, including Chapters II and III and paragraphs 6 to 9 thereof, to the extent applicable to the Company having regard to its classification as a Base Layer NBFC with an asset size below Rs. 500 Crore.

4. ROLE OF THE BOARD OF DIRECTORS

The Board of Directors ("the Board") shall have overall oversight of the Company's information technology, information security and cybersecurity framework and shall:

i. Approve this Policy and any material amendments.
ii. Review this Policy and the Company's technology and cybersecurity framework at least annually.
iii. Ensure that appropriate measures safeguard the Company's business information and financial records.
iv. Review periodic reports on the implementation and effectiveness of this Policy.
v. Ensure that arrangements for data backup, recovery and business continuity are in place and tested.
vi. Provide guidance on significant information security risks and deficiencies identified during reviews.
vii. Ensure compliance with applicable RBI Directions and other statutory and regulatory requirements.

The Board may delegate day-to-day implementation and monitoring of this Policy to an appropriate officer such delegation shall not absolve the Board of its overall oversight responsibility.

5. INFORMATION TECHNOLOGY SYSTEMS

The Company shall maintain IT systems appropriate to the nature and scale of its operations to support its business operations, accounting, financial reporting, record-keeping and regulatory compliance and shall prioritise basic IT systems that digitise and secure its primary business databases.

The Company's IT systems shall facilitate:

a. Accurate recording and maintenance of financial and operational information.
b. Secure storage and retrieval of business records.
c. Preparation of financial and management reports.
d. Timely preparation and submission of regulatory returns to RBI.
e. Appropriate access restrictions and segregation of duties.
f. Availability of information necessary for business continuity.

The Company shall maintain an inventory of its material IT assets, applications and data repositories, and shall periodically assess the adequacy of its IT systems and related controls, having regard to changes in business operations, regulatory requirements, and emerging technology risks and cyber threats.

6. ACCESS CONTROL AND USER MANAGEMENT

The Company shall establish physical and logical access controls to protect its IT infrastructure and information assets against unauthorised access. The following measures shall be implemented, as applicable:

a) Access to IT systems shall be granted only to authorised users.

b) Access rights shall be assigned according to the user's role, responsibilities and business requirements, on a least-privilege basis.

c) Each authorised user shall have a unique user ID wherever the relevant system supports it.

d) Password requirements, including complexity, confidentiality and secure handling, shall be defined and enforced.

e) Passwords and authentication credentials shall not be shared.

f) Access rights shall be reviewed periodically and modified or revoked promptly when a user's role changes or engagement ceases.

g) Administrative privileges shall be restricted to authorised personnel.

h) Unauthorised installation or use of software and applications is prohibited.

i) Physical access to computers, servers, storage devices and other critical equipment shall be restricted to authorised persons.

j) Unauthorised access attempts and material changes to access privileges shall be investigated and documented, wherever appropriate.

7. USER ROLES AND MAKER-CHECKER CONTROLS

7.1 The Company shall implement maker-checker controls for financial transactions, accounting entries, changes to critical records, regulatory submissions and other sensitive activities, wherever appropriate and technically feasible.

7.2 The person initiating a transaction, entry or change shall, wherever practicable, be different from the person authorising or approving it.

7.3 Where system limitations prevent automated maker-checker controls, alternative controls, including documented independent verification and approval, shall be implemented.

7.4 Any exception to maker-checker controls shall be justified, authorised and documented.

7.5 The Company shall periodically review the effectiveness of maker-checker arrangements to minimise errors, fraud and unauthorised changes.

8. INFORMATION SECURITY AND CYBERSECURITY

The Company shall implement information security and cybersecurity measures to protect its information assets and technology infrastructure against unauthorised access, disclosure, alteration, destruction, malware, phishing, ransomware and other cyber threats. Such measures shall include, as applicable:

i. Installation and maintenance of antivirus and endpoint protection software.

ii. Timely application of security patches and software updates.

iii. Use of supported operating systems and software.

iv. Protection of systems against malware, ransomware, phishing and other cyber threats.
v. Restriction of unauthorised access to business information and applications.
vi. Secure handling and storage of confidential business information.
vii. Appropriate controls over the use of removable storage devices.
viii. Secure configuration of computers and other IT equipment.
ix. Monitoring of suspicious activities and unauthorised attempts to access information systems.

The Company shall take reasonable measures to prevent unauthorised disclosure or misuse of confidential financial, corporate, employee and other business information. Any suspected compromise of an IT system, user account or information asset shall be reported promptly to the designated officer responsible for IT and information security. The Company shall periodically assess its cybersecurity risks and implement proportionate remedial measures.

9. PROTECTION OF DATA AND BUSINESS RECORDS

The Company shall maintain arrangements for protecting its business information, financial records, statutory registers, regulatory records and other important documents. Access to confidential information shall be restricted to persons who require such access for legitimate business purposes.

The Company shall endeavour to ensure that:

i. Business records are maintained accurately and completely.
ii. Confidential information is not disclosed to unauthorised persons.
iii. Important records are protected against accidental deletion, alteration or loss.
iv. Electronic records can be retrieved when required for business, statutory, regulatory or audit purposes.
v. Appropriate safeguards are applied when information is transmitted electronically.
vi. Data is retained and disposed of in accordance with applicable legal and regulatory requirements.

Employees and authorised users shall not copy, disclose, transfer or otherwise use Company information for unauthorised purposes.

10. DIGITAL SIGNATURE CERTIFICATES AND ELECTRONIC FILINGS

The Company shall use Digital Signature Certificates (DSCs) wherever required for electronic authentication, statutory filings, regulatory submissions and other applicable electronic transactions.

The Company shall ensure that:

i. DSCs are obtained and used only by duly authorised persons.
ii. Private keys, tokens, passwords and other authentication credentials are kept confidential.
iii. DSCs are not used by unauthorised persons.
iv. The validity of DSCs is monitored and timely renewal is undertaken wherever required.
v. Electronic filings and submissions are reviewed and authorised by appropriate personnel before submission.
vi. Electronic acknowledgements and filing records are retained for future reference.

The Company shall maintain controls over the preparation, verification and submission of regulatory returns to RBI and other statutory authorities.

11. MANAGEMENT INFORMATION SYSTEMS (MIS) AND REGULATORY REPORTING

The Company's IT systems shall support the generation and maintenance of reliable financial information, management reports and regulatory data. The Company shall endeavour to maintain system-generated reports, as appropriate to its operations, covering:

i. Financial position and business performance.
ii. Income, expenses and other material financial information.
iii. Relevant business and operational indicators.
iv. Information required for management decision-making.
v. Information necessary for applicable RBI returns and other statutory or regulatory filings.

Reports and information used for financial reporting and regulatory submissions shall be checked for accuracy and completeness by authorised personnel. The Company's IT arrangements shall support submission of regulatory returns within the prescribed timelines.

12. DATA BACKUP AND RECOVERY

12.1 Business-critical data, including accounting records, statutory registers and regulatory filings, shall be backed up at regular intervals, with the frequency determined by the criticality of the data.

12.2 Backups shall be stored securely, with at least one copy maintained separately from the primary system (for example, offline, offsite or in a secure cloud environment), and protected against unauthorised access and tampering.

12.3 Restoration of backups shall be tested at least annually, and the results documented.

12.4 Backup media and data that are no longer required shall be disposed of securely.

13. BUSINESS CONTINUITY PLAN (BCP)

13.1 The Company shall maintain a BCP, proportionate to its size and operations, that identifies critical business functions and systems, recovery priorities, responsible personnel and communication arrangements.

13.2 The BCP shall address, at minimum, loss of IT systems or data, cyber incidents, unavailability of premises or personnel, and failure of third-party service providers.

13.3 The BCP shall be tested at least annually, with results documented, shortcomings remediated, and a report placed before the Board.

13.4 The BCP shall be reviewed at least annually and whenever there is a significant change in the Company's operations or IT environment.

14. IT RISK ASSESSMENT

The Company shall assess risks associated with its IT systems at least annually, proportionate to the nature and complexity of its operations. The assessment shall consider, as applicable:

- Threats to information systems and business data.
- Vulnerabilities arising from outdated software or inadequate security controls.
- Risks of unauthorised access and misuse of user privileges.
- Risks of data loss, corruption or unauthorised alteration.
- Risks arising from cyberattacks, malware and phishing.
- Risks associated with third-party IT service providers.
- Risks of system failure, disruption or unavailability.
- Adequacy of existing backup and recovery arrangements.

The assessment shall identify material risks, existing controls and areas requiring improvement. The findings shall be documented and placed before the Board for review.

Corrective measures shall be implemented within documented timelines, taking into account the severity and potential impact of the identified risks.

15. INFORMATION SECURITY AWARENESS AND TRAINING

The Company shall promote awareness of information security and cybersecurity risks among its directors, employees and other relevant users covering, as appropriate:

- Password security and access control.
- Identification of phishing emails and fraudulent communications.
- Safe use of email, internet and business applications.
- Protection of confidential business information.

- Secure handling of DSCs and electronic filing credentials.
- Reporting of suspected security incidents.
- Prevention of unauthorised disclosure or misuse of Company information.

The Company shall organise awareness or familiarisation programmes for the Board and senior management regarding significant cybersecurity risks and relevant developments. Training and awareness activities shall be conducted at least annually and shall be proportionate to the Company's size, operational requirements and risk profile.

16. MONITORING AND COMPLIANCE

The designated officer assigned responsibility for IT and information security shall monitor the implementation of this Policy. Material non-compliance, significant vulnerabilities, major system failures and cybersecurity incidents shall be escalated to the Board.

The Company shall maintain records of:

- IT systems and authorised users.
- Access rights and material access changes.
- Backup and restoration activities.
- Significant cybersecurity incidents and corrective actions.
- IT risk assessments and remediation measures.
- Relevant training and awareness activities.
- Periodic reviews of this Policy and the BCP.

Where deficiencies are identified, corrective measures shall be undertaken within a reasonable and documented timeframe.

17. POLICY REVIEW AND AMENDMENTS

This Policy shall be reviewed by the Board at least once every year and whenever required due to:

- Changes in applicable RBI directions or other legal requirements.
- Significant changes in the Company's business activities or IT infrastructure.
- Findings from risk assessments, audits or other reviews.
- Any other circumstance warranting revision.

Any amendment shall be placed before the Board for approval.

APPROVAL AND EFFECTIVE DATE

This Policy was placed before and approved by the Board of Directors of HB Stockholdings Limited at its meeting held on 05th November, 2026 and shall come into effect from 05th November, 2026. The Policy shall remain in force until amended or replaced by the Board.

****