KYC & AML POLICY
Supergrowth Investments Private Limited

1. INTRODUCTION, PURPOSE AND SCOPE

1.1 This Know Your Customer and Anti-Money Laundering Policy (**"Policy"**) sets out the framework, principles and procedures adopted by Supergrowth Investments Private Limited (**"Company"**) for the identification of customers, customer due diligence, and the prevention of money laundering and terrorist financing in the conduct of its business.

1.2 This Policy applies to the identification of customers, customer due diligence, and the prevention of money laundering and terrorist financing in connection with any customer-facing, onboarding, servicing or related function that the Company performs in connection with the provision of credit or related services, whether on its own account or for or on behalf of one or more banks or non-banking financial companies (**"Partner RE"**).

1.3 The obligations of customer due diligence, reporting and record-keeping under the PMLA and the RBI KYC Directions apply to reporting entities and to regulated entities. The Company shall comply with those obligations to the extent that they apply to it and, where the Company performs functions for or on behalf of a Partner RE, shall operate so as to enable and support that Partner RE's compliance with Applicable Law. The Company adopts this Policy in order to:

(a) identify and verify its customers and, where applicable, their beneficial owners, and carry out customer due diligence, in a manner consistent with Applicable Law and with any Partner RE's board-approved KYC policy that applies;

(b) enable risk-based monitoring of customer activity and the timely escalation or reporting of unusual or suspicious activity;

(c) ensure the confidentiality, security, retention and lawful processing of customer information;

(d) screen customers against the applicable sanctions and designated-persons lists; and

(e) maintain sound anti-money laundering and counter-terrorist-financing standards in the Company's dealings, including with its vendors, agents and counterparties.

1.4 This Policy applies to all directors, officers and employees of the Company, and to all agents, sub-contractors and service providers engaged by the Company, who are involved in any function to which this Policy applies. Where the Company performs functions for or on behalf of a Partner RE, this Policy is to be read together with that Partner RE's board-approved KYC/AML policy, and, in the event of any conflict, the stricter of that policy and Applicable Law shall prevail.

2. DEFINITIONS

2.1 In this Policy, unless the context otherwise requires:



(a) **"Applicable Law"** means any statute, rule, regulation, direction, notification, order, guideline or policy of any Governmental Authority having jurisdiction over the matter in question, as amended from time to time, including the enactments referred to in Clause 3;

(b) **"Beneficial Owner"** means the natural person who ultimately owns or controls a customer or on whose behalf a transaction is conducted, determined in accordance with Rule 9 of the PML Rules;

(c) **"CDD"** or **"Customer Due Diligence"** means the identification and verification of a customer and, where applicable, its Beneficial Owner, and the ongoing scrutiny of the customer relationship, in accordance with this Policy and the RBI KYC Directions;

(d) **"Customer"** means a person whom the Company onboards or services, or who applies to be onboarded or serviced, in connection with the provision of credit or a related service to which this Policy applies;

(e) **"Designated Director"** and **"Principal Officer"** have the meanings given under the PMLA and the PML Rules, and refer to the officers appointed by a Partner RE in that capacity;

(f) **"Digital Lending App"** or **"DLA"** means a mobile or web-based application operated by or on behalf of the Company that facilitates digital lending, as described in the RBI Digital Lending Directions;

(g) **"FIU-IND"** means the Financial Intelligence Unit – India;

(h) **"Governmental Authority"** means any government or statutory, regulatory, judicial or quasi-judicial authority having jurisdiction over the Company, including the Reserve Bank of India;

(i) **"Lending Service Provider"** or **"LSP"** means an agent of a regulated entity that performs one or more of the regulated entity's digital lending functions, as defined in the RBI Digital Lending Directions;

(j) **"Officially Valid Document"** or **"OVD"** has the meaning given under the RBI KYC Directions;

(k) **"PEP"** or **"Politically Exposed Person"** means an individual who is or has been entrusted with prominent public functions in India or a foreign country, and includes such person's family members and close associates, as described in the RBI KYC Directions;

(l) **"Partner RE"** means a bank or non-banking financial company for or on behalf of whom the Company performs any function to which this Policy applies, being Ratnaafin Capital Private Limited and Mufin Green Finance Limited;

(m) **"PMLA"** means the Prevention of Money-Laundering Act, 2002, and **"PML Rules"** means the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, in each case as amended;



(n) **"RBI KYC Directions"** means the Reserve Bank of India (Non-Banking Financial Companies – Know Your Customer) Directions, 2025, as amended from time to time;

(o) **"RBI Digital Lending Directions"** means the Reserve Bank of India (Digital Lending) Directions, 2025, as amended;

(p) **"Suspicious Transaction"** has the meaning given under the PML Rules; and

(q) **"V-CIP"** means video-based customer identification process as permitted under the RBI KYC Directions.

3. REGULATORY FRAMEWORK

3.1 This Policy is framed with reference to, and is to be operated consistently with, the following (as amended from time to time), to the extent applicable to the Company's activities:

(a) the PMLA and the PML Rules;

(b) the RBI KYC Directions;

(c) the RBI Digital Lending Directions;

(d) the RBI guidelines on outsourcing of financial services and on outsourcing of information-technology services (**"Extant Outsourcing Guidelines"**);

(e) the Unlawful Activities (Prevention) Act, 1967 (including the procedure under Section 51A) and the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005, and the orders and lists issued thereunder;

(f) the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025; and

(g) where applicable, each Partner RE's board-approved KYC/AML policy and the terms of the Company's arrangements with each Partner RE.

4. GOVERNANCE AND RESPONSIBILITY

4.1 Board oversight

The Board of Directors of the Company (the **"Board"**) is responsible for approving this Policy and for overseeing its implementation. The Board shall review the adequacy and effectiveness of the Company's KYC/AML controls at least once each financial year.

4.2 Administration of this Policy

The Company shall be responsible for the day-to-day administration of this Policy, for maintaining liaison with any relevant Partner RE's Designated Director and Principal Officer, for receiving and assessing internal reports of unusual or suspicious activity, and for ensuring staff training and



record-keeping. The Company shall designate a person to liaise with each Partner RE's Principal Officer.

4.3 **Cooperation with Partner REs**

Where the Company performs any function for or on behalf of a Partner RE, the Company shall perform that function in accordance with the Partner RE's board-approved KYC policy, shall provide the Partner RE and its auditors and the Reserve Bank of India with access to relevant records and premises as required, and shall promptly furnish such information and reports as the Partner RE requires to discharge its obligations under Applicable Law.

4.4 **Future status**

If the Company at any time itself becomes a reporting entity under the PMLA, or a regulated entity, it shall register with FIU-IND, appoint a Designated Director and a Principal Officer, and amend this Policy to give effect to the resulting obligations, including direct reporting to FIU-IND.

5. CUSTOMER ACCEPTANCE

5.1 The Company shall not onboard, and shall not permit the continuation of, a customer relationship where:

(a) the customer is anonymous or is identified by a fictitious or benami name;

(b) the identity of the customer or its Beneficial Owner cannot be verified, or the required CDD cannot be completed due to non-cooperation of the customer or unreliability of the documents or information furnished by the customer; in such circumstances, the Company shall consider filing a suspicious transaction report (STR), where necessary;

(c) the customer, its Beneficial Owner or any connected person appears on a sanctions or designated-persons list referred to in Clause 8;

(d) there is reason to believe that the relationship or transaction is intended to be used for money laundering, terrorist financing or any other unlawful purpose; or

(e) the customer declines to provide, or provides information the Company has reason to believe is false, in respect of the CDD required.

5.2 Each customer shall be assigned a risk category under Clause 7 at the time of onboarding. The Customer Acceptance Policy shall not result in denial of a financial facility to members of the general public, especially those who are financially or socially disadvantaged, including Persons with Disabilities (PwDs). The Company shall not reject an application for onboarding or periodic updation of KYC without application of mind. The officer concerned shall duly record the reason(s) for such rejection.

6. CUSTOMER IDENTIFICATION AND DUE DILIGENCE

6.1 **When performed**



Customer identification and CDD shall be carried out at the commencement of an account-based relationship with the customer; when carrying out any international money transfer operations for a person who is not an account-based customer of the Company; when carrying out an occasional transaction for a non-account-based customer where the amount involved is equal to or exceeds Rs. 50,000 (Rupees Fifty Thousand), whether as a single transaction or several transactions that appear to be connected, or where the Company has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below that threshold; when selling third-party products as an agent, selling its own products, or providing any other product or service, for an amount exceeding Rs. 50,000 (Rupees Fifty Thousand); when there is a material change in the customer's profile or ownership; when there is a doubt about the authenticity, veracity or adequacy of the customer identification data or information previously obtained; and on a periodic basis under Clause 9. The Company shall not seek any introduction while opening an account or commencing a customer relationship.

6.2 **Individuals**

For an individual customer (including a sole proprietor or individual guarantor), the Company shall obtain and verify an OVD and the Permanent Account Number (or Form 60), together with a recent photograph. Identification and verification may be carried out through Aadhaar-based e-KYC (with Aadhaar numbers redacted/masked and handled in accordance with the Aadhaar framework), V-CIP, the Central KYC Records Registry, or physical/scanned OVDs, in each case as permitted under and subject to the limits of the RBI KYC Directions. Where an individual is onboarded on a non-face-to-face basis using Aadhaar OTP-based e-KYC, the relationship shall be subject to the enhanced monitoring and transaction limits prescribed under the RBI KYC Directions, including that the aggregate amount of term loans sanctioned to such a customer shall not exceed Rs. 60,000 (Rupees Sixty Thousand) in a year, and full customer due diligence shall be completed within one year of onboarding. Equivalent electronic documents (including documents obtained through the Digital Locker facility) may be accepted as Officially Valid Documents to the extent permitted under the RBI KYC Directions. Where V-CIP is used, it shall replicate a real-time, face-to-face interaction, require the customer to be physically present in India, employ liveness detection (provided that specific facial gestures, such as blinking, smiling or frowning, shall not be mandatory, and the process shall not exclude persons with disabilities or special needs), and the V-CIP activity log and recordings shall be stored in systems located in India and shall not be retained on any third-party system.

6.3 **Legal entities.**

For a customer that is a company, partnership firm, limited liability partnership, trust, society, association of persons or Hindu undivided family, the Company shall obtain and verify its constitutional and registration documents, its Permanent Account Number, and the identity and authority of the natural person(s) authorised to act on its behalf (including the relevant board resolution or power of attorney).

6.4 **Beneficial ownership**

For every non-individual customer, the Company shall identify and take reasonable steps to verify the Beneficial Owner(s) in accordance with Rule 9 of the PML Rules, including the controlling ownership-interest thresholds prescribed thereunder, and shall identify the natural person exercising control where no such person is otherwise identified. The applicable beneficial-

ownership thresholds are those currently prescribed under the PML Rules and the RBI KYC Directions, as amended from time to time (including, as reduced by the 2023 amendments to the PML Rules, a controlling-ownership-interest threshold of more than ten per cent of the shares, capital or profits for companies and for partnership firms, and an interest of ten per cent or more for trusts; the threshold for unincorporated associations or bodies of individuals remains more than fifteen per cent).

6.5 **CKYC**

The Company shall, in coordination with the relevant Partner RE, retrieve and upload KYC records to the Central KYC Records Registry as required under the RBI KYC Directions.

6.6 **Reliance and outsourcing**

Where the Company relies on customer due diligence carried out by a Partner RE or another third party, such reliance shall be permitted only within the limits of the RBI KYC Directions and the Extant Outsourcing Guidelines, and the ultimate responsibility of the relevant reporting entity for customer due diligence shall not be affected.

7. RISK CATEGORISATION

7.1 The Company shall categorise each customer as low, medium or high risk, based on a risk assessment that takes into account the type of customer, its ownership and control structure, its geographic location (including any nexus with jurisdictions identified by the Financial Action Task Force as high-risk or non-cooperative), the nature of the credit facility and delivery channel, the involvement of any PEP, and the customer's expected activity. The risk category shall determine the extent of CDD applied and the frequency of ongoing review, and shall be reviewed and updated periodically and upon any material change.

8. ENHANCED DUE DILIGENCE, PEPs AND SANCTIONS SCREENING

8.1 **Enhanced due diligence**

Enhanced due diligence shall be applied to high-risk customers, non-face-to-face relationships, complex or unusually large arrangements, and any relationship presenting a higher risk of money laundering or terrorist financing. Enhanced due diligence may include obtaining additional identification and ownership information, establishing the source of funds and, where relevant, source of wealth, and applying closer ongoing monitoring.

8.2 **Politically Exposed Persons**

Where a customer or Beneficial Owner is a PEP, the Company shall obtain senior-management approval to establish or continue the relationship, take reasonable measures to establish the source of funds and source of wealth, and subject the relationship to enhanced ongoing monitoring.

8.3 **Sanctions and designated persons**

The Company shall screen each customer, its Beneficial Owner(s) and connected persons, at onboarding and on an ongoing basis (including whenever the relevant lists are updated), against



the United Nations Security Council consolidated sanctions lists, the lists of individuals and entities designated under the Unlawful Activities (Prevention) Act, 1967, and the orders issued under the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005. The Company shall not establish or continue any relationship with, or process any transaction for, a designated person; and shall, in the event of a match, freeze onboarding, refrain from tipping-off, and immediately escalate to the relevant Partner RE and, as required, to the competent authority in accordance with the Section 51A procedure. The Company shall carry out such screening using appropriate name-screening technology, and shall screen its customer base on an ongoing basis, including screening against persons and entities newly designated under the applicable lists promptly upon each update, as required under the RBI KYC Directions.

9. ONGOING DUE DILIGENCE AND MONITORING

9.1 The Company shall monitor customer activity for consistency with the customer's risk profile and known business, and shall maintain risk-based rules and thresholds to identify unusual patterns, including transactions or activity inconsistent with the customer's known business or profile, circular or related-party fund flows, payments to or from apparently unrelated third parties, and transactions that appear structured to avoid applicable thresholds or reporting.

9.2 Alerts shall be reviewed by, or under the supervision of, the Company's senior management, and, where applicable, escalated to the relevant Partner RE.

9.3 Customer information shall be kept current, and periodic updation of KYC shall be carried out at the periodicity applicable to the customer's risk category under the RBI KYC Directions (as a guide, high-risk every two years, medium-risk every eight years and low-risk every ten years), or as otherwise required by the relevant Partner RE. In carrying out periodic updation, the Company may, where there is no change (or only a change of address), accept a self-declaration from the customer to the extent permitted under the RBI KYC Directions; shall give the customer prior intimation and the advance reminders required thereunder (including at least one reminder in physical form) before restricting an account for non-updation; and shall, with the customer's consent, fetch and update KYC records through the Central KYC Records Registry.

10. REPORTING OF SUSPICIOUS ACTIVITY

10.1 Any employee or agent of the Company who becomes aware of an activity or transaction that is, or may be, unusual or suspicious shall report it promptly to the Company's senior management. The Company's senior management shall assess each such report.

10.2 Where the Company is a reporting entity under the PMLA in respect of a matter, the Company's senior management shall ensure that the reports required under the PMLA and the PML Rules (including cash transaction reports and suspicious transaction reports) are filed with FIU-IND within the prescribed timelines. Where the Company performs functions for or on behalf of a Partner RE and is not itself the reporting entity in respect of the matter, the Company's senior management shall, without tipping-off the customer or any other person, promptly escalate the matter to the Principal Officer of the relevant Partner RE, together with all supporting information, so as to enable timely reporting to FIU-IND.



10.3 The Company and its personnel shall not disclose to the customer or to any unauthorised person the fact that a report has been or may be made, or that an investigation is being or may be carried out.

11. RECORD KEEPING AND RETENTION

11.1 The Company shall maintain records of customer identity and CDD, of the transactions processed through its platform, and of internal and escalated reports, in a manner that permits reconstruction and retrieval. Such records shall be retained for the periods required under the PMLA and the PML Rules (being, as a general rule, five years from the date of cessation of the customer relationship or the date of the transaction, as applicable) and for such longer period as the relevant Partner RE or Applicable Law requires. Records shall be kept confidential and secure, and shall be made available to any relevant Partner RE, and to auditors and the Reserve Bank of India, to the extent required by Applicable Law or by the Company's arrangements with the Partner RE.

12. DATA PROTECTION AND CONFIDENTIALITY

12.1 The Company shall collect, use, store, transfer and delete customer personal data in accordance with the Digital Personal Data Protection Act, 2023 and the rules made thereunder, and with the data-governance requirements of the RBI Digital Lending Directions.

12.2 Data collection shall be need-based and supported by the customer's prior, explicit consent with an audit trail. To the extent the RBI Digital Lending Directions apply to the Company, any access by a digital lending application operated by or on behalf of the Company to a device's camera, microphone or location shall be limited to a one-time requirement for onboarding or KYC; access to other device resources such as files, media, contacts and call logs is prohibited; and biometric data shall not be stored except where expressly permitted by Applicable Law.

12.3 To the extent the RBI Digital Lending Directions apply to the Company, customer data shall be stored on servers located in India, and where any such data is processed outside India, it shall be brought back to India and deleted from servers outside India within twenty-four (24) hours of processing.

12.4 The Company shall maintain and publicly disclose a privacy policy, implement reasonable security safeguards, and ensure that customer information and KYC data are used only for the purpose for which they were collected. Directors, officers, employees and agents of the Company shall maintain the confidentiality of customer information.

13. TRAINING AND AWARENESS

13.1 The Company shall provide periodic, role-appropriate training to its employees and agents on this Policy, on the identification and handling of unusual and suspicious activity, on sanctions screening, and on data-protection requirements, and shall maintain records of such training.

14. OUTSOURCING AND SUB-CONTRACTING



14.1 Where the Company engages any agent, sub-contractor or other service provider to perform any function under this Policy, it shall carry out due diligence on such provider, impose back-to-back obligations consistent with this Policy and the Extant Outsourcing Guidelines, and remain responsible for the acts and omissions of such provider. Where the Company performs functions for or on behalf of a Partner RE, any function that the Partner RE is required to retain shall not be outsourced by the Company.

15. AUDIT AND MONITORING

15.1 The Company's KYC/AML controls shall be subject to periodic independent testing as part of the Company's internal audit or compliance-testing arrangements, and the Company shall cooperate with any audit, review or inspection carried out by or on behalf of any relevant Partner RE or the Reserve Bank of India, to the extent applicable.

16. REVIEW AND AMENDMENT

16.1 The Board shall review this Policy at least once each financial year, and upon any material change in Applicable Law or in the Company's business or arrangements with Partner REs, and may amend, modify or replace it at any time. Any provision of this Policy that becomes inconsistent with Applicable Law shall, to the extent of such inconsistency, be deemed modified to conform to Applicable Law, and the remaining provisions shall continue in effect.

17. ADOPTION AND EFFECTIVE DATE

17.1 This Policy was approved and adopted by the Board of Directors of the Company, and is effective since 2000. The latest review of this Policy was carried out on 30 April 2026.

