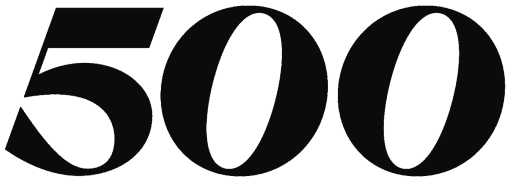

500 STARTUPS MANAGEMENT COMPANY, L.L.C.

CODE OF CONDUCT
&
COMPLIANCE MANUAL

December 15, 2021

CONTENTS

OVERVIEW OF 500 GLOBAL'S COMPLIANCE POLICIES AND PROCEDURES

This Code of Conduct and Compliance Manual (the "**Manual**") is intended to apply to all employees, contractors, consultants, general partners or other personnel of 500 Startups Management Company, L.L.C. (the "**Firm**") and all affiliated entities including but not limited to all direct and indirect subsidiaries of the Firm, 500 Startups Incubator, L.L.C and all Funds advised by the Firm (together "**500 Global**"), it being clarified that the Manual shall apply to all entities which enter into a contractual arrangement with the Firm (or it's affiliate) whereby such entity agrees that the Manual shall apply with respect to such entity, as well as its employees, contractors, consultants, general partners or other personnel.

Compliance Officer
Brinda Dutta is the Firm's "Compliance Officer" for all purposes of this Manual and any questions or concerns about anything raised in this Manual should be directed to her at compliance@500.co.

Following the resignation or removal of the current Compliance Officer, the Firm shall as soon as reasonably practicable appoint another person as the new Compliance Officer.

Reporting Violations
Employees should report any violation of this Manual to the Compliance Officer. Any question concerning the applicability of the provisions of this Manual to a particular situation should be addressed to the Compliance Officer. Failure to report a violation to the Compliance Officer may result in disciplinary action against any Employee, which may include termination of employment.

Whistleblower Policy
It is imperative to the effectiveness of the Firm's compliance program that Employees have the opportunity to report any concerns or suspicions of improper activity at the Firm confidentially and without retaliation.

The Firm will take seriously any report regarding a potential violation of any policy or other improper or illegal activity, and recognizes the importance of keeping the identity of the reporting person from being widely known. Employees should be assured that the Firm will appropriately manage all such reported concerns or suspicions of improper activity in a timely and professional manner and without retaliation.

Policy Coverage
The Firm's Whistleblower Policy covers the treatment of all concerns or complaints relating to potential violations of Securities laws or suspected improper activity in the preparation of

financial statements, disclosures, accounting practices, internal controls or other auditing matters, including but not limited to the following:

- use of the Firm's resources for the personal benefit of anyone other than the Firm;
- improper trading activities including trading for his or her personal account misusing non-public information;
- receipt of excessive gifts, entertainment, or other consideration from persons doing business with the Firm;
- use the Firm's resources, or making payments of any kind, for the benefit of any government, government official, financial institution or employee thereof, or industry official with the intent of inducing or influencing the recipient to misuse his or her position;
- paying or giving, offering or promising to pay, or authorizing or approving such offer or payment of any funds, gifts, services or anything else of any value, to any foreign official or other person that would be a "Covered Person" as defined in the Anti-corruption and Bribery Policy on page 34, or the purpose of obtaining or retaining business, favorable treatment, or other commercial benefits, whether by (i) influencing any act or decision of the Covered Person in his official capacity; (ii) inducing the Covered Person to do or not do any act in violation of his lawful duty; or (iii) inducing the Covered Person to use his influence to that end with a foreign government or instrumentality (see the Anti-corruption and Bribery Policy on page 34 for more detail).
- fraud or deliberate error in the preparation, evaluation, review or audit of any financial statement of the Firm;
- fraud or deliberate error in the recording and maintaining of financial records of the Firm;
- deficiencies in or non-compliance with the Firm's internal accounting controls;
- misrepresentations or false statement to or by a senior officer or accountant regarding a matter contained in the financial records, financial reports or audit reports of the Firm;
- deviation from full and fair reporting of the Firm's financial situation; and
- the retaliation, directly or indirectly, or engagement of others to do so, against anyone who reports a potential violation of the Securities laws or violation of this Manual.

Responsibility of the Whistleblower

Employees should be acting in good faith in reporting a complaint or concern under this policy and must have reasonable grounds for believing a deliberate misrepresentation has been made regarding accounting or audit matters or a breach of this Manual. A malicious allegation known to be false is considered a serious offense and will be subject to disciplinary action which may include termination of employment.

Handling of Reported Improper Activity

Employees should promptly report suspected improper activity to the Compliance Officer to enable the matter to be investigated. Employees may report suspected improper activity by the Compliance Officer to the Firm's management.

Anonymous Reporting

Employees may report suspected improper activity to the Compliance Officer by filing an Improper Activity Report using this form available on the Compliance team site. Concerns about improper activity by the Compliance Officer or his/her staff may be reported to any member of the Firm's management using an Improper Activity Report. An Improper Activity Report should be complete and provide detail as to the person or persons involved, the specific nature of the suspected improper activity and the time or times the activity was to have taken place. Incomplete Improper Activity Reports may prevent the Compliance Officer and/or Firm's management to properly investigate the report and may therefore not necessarily afford the Employee the protections of this policy.

No Retaliation Policy

It is the Firm's policy that no Employee who submits a complaint made in good faith will experience retaliation, harassment, or unfavorable or adverse employment consequences. Any Employee who retaliates against a person reporting a complaint will be subject to disciplinary action, which may include termination of employment. An Employee who believes they have been subject to retaliation or reprisal as a result of reporting a concern or making a complaint is to report such action to the Compliance Officer.

New Policies

In addition to the policies and procedures set out in this Manual, each Employee may be subject to certain other Firm policies and/or procedures established from time-to-time. In the event such policy is adopted, each Employee to whom the policy relates will be asked to review and sign the policy (however failure to so sign shall not affect the effectiveness of the policy as it pertains to such Employee).

Employee's responsibility

It is an Employee's responsibility to read and familiarize themselves with the policies and procedures contained in this document. Employees will be required to provide an executed copy of the Certificate of Acknowledgement and Agreement in Exhibit A on page 48 upon publication of this Manual. All new Employees joining the Firm after the date of publication will submit their Certificate during the Firm's HR onboarding process.

Any failure to comply with the policies and procedures outlined herein may result in an Employee's discipline or dismissal as well as the possible imposition of criminal, civil or administrative penalties. **EMPLOYEES MUST TAKE COMPLIANCE SERIOUSLY.**

Additional Approvals for Senior Management

In addition to the processes set out herein, certain members of the Firm's senior management may also be required to seek prior consent of the Board of Officers or its committees for approval of any waivers of any matters set out in this Compliance Manual. Affected Employees should submit any requests via the usual channels but note that the Board of Officers has up to 5 working days from receipt to determine their response. If any Employee has any questions or concerns about such additional approvals please refer them to the Compliance Officer.

Conflict with local non-US laws, rules or regulations

To the extent that any provision of this Manual, conflicts with the provisions of any applicable statute, law, ordinance, or regulation (collectively, the "**Law**") that the Firm or any Employee is subject to ("**Local Law Obligation**"), the Local Law Obligation shall to the fullest extent permitted by law, prevail. Should any provision of this Manual become or deemed to be invalid, illegal or unenforceable in any applicable jurisdiction by reason of the scope, extent or duration of its coverage, then such provision shall be deemed amended to the minimum extent necessary to conform to applicable law so as to be valid and enforceable or, if such provision cannot be so amended without materially altering the intention of the Firm, then such provision shall be stricken and the remainder of this Manual shall continue in full force and effect. If any provision of this Manual is rendered illegal by any present or future Law then that provision shall be curtailed or limited only to the minimum extent necessary to bring the provision into compliance with the Law. If any Employee has any questions or concerns about such conflict please refer them to the Compliance Officer.

Thematic Funds

Employees who are also managers of any of the Firm's "thematic funds" ("Thematic Fund Managers") may also be required to comply with applicable Local Law Obligations and additional compliance policies and procedures related to management and operation of those funds as published or notified by the Firm or its Affiliates from time to time.

Definitions

Unless the context requires otherwise, the following terms used throughout this Manual shall have the following meanings:

Affiliate: means any person or entity controlling, controlled by, or under direct or indirect common control with such person or entity including the Funds.

Compliance Officer: means Brinda Duttaor such other Compliance Officer as may be appointed by Firm management from time to time.

Firm: means 500 Startups Management Company, L.L.C. and all affiliated entities including but not limited to all direct and indirect subsidiaries of the Firm, 500 Startups Incubator, L.L.C and all Funds advised by the Firm.

Funds*:* means any investment fund advised by the Firm including but not limited to any global fund, thematic fund, accelerator fund, managed account or SPV.

Employees: means all employees and other personnel of the Firm, to include those persons who serve as members, managers, officers or employees or contractors of the Firm and the direct and indirect individual constituent partners, members, officers, contractors and directors of not only the Firm but also each entity Affiliated with the Firm that serves as the general partner or management company (or in a similar capacity) to any of the Firm's family of investment Funds, regardless of whether such person is technically an employee of the Firm or such entity for the purposes of federal, state or local law.

United States: means the United States of America.

500 GLOBAL CODE OF CONDUCT

The Firm will promote and require ethical conduct by all officers and Employees.

Ethical Conduct

This ethical conduct includes, but is not limited to, the following:

- maintain honesty and integrity, avoiding actual or apparent conflicts of interest in personal and professional relationships;
- provide colleagues, business partners and investors with information that is accurate, complete, objective, relevant, timely, and understandable;
- reasonably comply with all applicable rules and regulations of federal, state, provincial, and local governments, and other appropriate private and public regulatory agencies;
- act in good faith, responsibly, with due care, competence and diligence, without misrepresenting material facts or allowing one's independent judgment to be subordinated;
- respect the confidentiality of information acquired in the course of one's work except when authorized or otherwise legally obligated to disclose. Confidential information acquired in the course of one's work will not be used for personal advantage;
- share knowledge and maintain skills important and relevant to one's job;
- diversity is a fundamental part of who we are, embrace it;
- proactively promote ethical behavior as a responsible partner among peers, in the work environment and the community;
- achieve responsible use of and control over all assets and resources employed or entrusted; and
- be accountable for adhering to this Code.

Within the venture capital industry, the Firm is judged on the collective and individual actions of its partners, managers and Employees. Each Employee must manage their personal and business affairs so as to avoid situations that might lead to a conflict or even suspicion of a conflict between them and their duties to the Firm, its business partners, and its investors. An Employee's position must never be used, directly or indirectly, for private gain, to advance personal interest, or to obtain favors or benefits for themselves, family members, or anyone else.

The purpose of this Code is to reiterate the high standard of conduct that is associated with ethical business practices and to identify areas and situations where public trust and confidence might be compromised or a law violated and to set forth guidelines governing such situations.

Ethical, moral and legal behaviors are the responsibilities of the individual employee. The Firm will not expect anyone in its employ to perform an act contrary to ethical or moral standards or to any laws or regulations.

The following conduct is prohibited and will not be tolerated by the Firm. This list of prohibited conduct is illustrative only; other types of conduct that threaten security, personal safety, employee welfare and Firm operations also may be prohibited:

- falsifying employment records, employment information, or other Firm records;
- theft and deliberate or careless damage or destruction of any Firm property, or the property of any employee or client;
- removing or borrowing Firm property without prior authorization;
- unauthorized use of Firm equipment, time, materials, or facilities;
- provoking a fight or fighting during working hours or on Firm property;
- carrying firearms or any other dangerous weapons on Firm premises, or while conducting Firm business, at any time;
- engaging in criminal conduct whether or not related to job performance;
- causing, creating, or participating in a disruption of any kind during working hours on Firm property;
- insubordination, including but not limited to failure or refusal to obey the orders or instructions of a manager or member of management, or the use of abusive or threatening language toward a manager or member of management;
- failing to notify a manager when unable to report to work;
- unreported absence of three consecutive scheduled workdays;
- violating any safety, health, security or Firm policy, rule, or procedure;
- committing a fraudulent act or a breach of trust under any circumstances;
- committing of or involvement in any act of harassment, discrimination or intimidation of another individual;
- abuse of human rights laws, or working with partners who do;
- partaking in forced and compulsory labor or child labor or working with partners who do;
- discrimination during the course of recruiting and/or promotion of Employees;
- dealing with any investors or investments that may involve money laundering or terrorist financing or where there are any suspicions with regard to the origin of any funds; and
- being corrupt, taking a bribe, or extortion.

This statement of prohibited conduct does not alter the terms of the Firm's policy of at-will employment for US employees. Either of an Employee or the Firm remains free to terminate the employment relationship in accordance with the terms of that Employee's contract.

Employees are also referred to the Firm's Sexual Harassment Policy, any questions on which should be directed to the HR Department.

Regulatory Compliance Policies and Procedures

Rule 506 of Regulation D under the Securities Act of 1933 contains certain provisions and rules providing exemptions from registration requirements. In order to maintain compliance with the SEC, each Employee will, upon joining the Firm and periodically thereafter be asked to

complete a "Bad Actor" Questionnaire. Giving falsified or misleading information on the questionnaire may lead to civil or criminal penalties.

Additionally, each Employee may be subject to certain other Firm policies and/or procedures established from time-to-time. In the event such policy is adopted, each Employee to whom the policy relates will be asked to review and sign the policy (however, failure to so sign shall not affect the effectiveness of the policy as it pertains to such employee).

Protection of Confidential Information

Protection of the Firm's information is the key to the continued success of the Firm. It is in the best interest of the survival and growth of the Firm to maintain maximum security for all proprietary information and industry developments shared or initiated by the Firm's workforce.

Employees will have access to proprietary and confidential information, all Firm and Affiliate business must be kept strictly confidential.

Another critical responsibility is to maintain the trust placed with the Firm by the Firm's business partners and investors. Confidential information, whether obtained from business partners of the Firm or its Affiliates does business, or from sources within the Firm, must be safeguarded. Confidentiality is important regardless of the form the information takes, whether oral, in print, or on electronic media.

Employees must take care in what is said, to whom, and where, about how documents, files, reports and the information displayed on computer screens are treated as well as social media sites. Employees are also responsible for the internal security of such information. Disclosures of sensitive investor personal information or non-public portfolio company valuation information are two areas of particular concern in the Firm's business.

Confidential or proprietary information described above includes information for the Firm, its business partners and investors, and all of its Affiliates and the other entities through which the Firm conducts its business.

POLICY REGARDING POLITICAL CONTRIBUTIONS

December 15, 2021

Policy Statement

It is the unconditional policy of the Firm to comply with all applicable laws and regulations that restrict or regulate investment advisers and their personnel from engaging in political contributions and fundraising activities. This Policy mandates that all Firm Employees and their

immediate family members refrain from making political contributions or engaging in political fundraising activities in the United States except to the extent explicitly permitted in this Policy. The consequences of non-compliance with this Policy could result in discipline or dismissal of an Employee, as well as the imposition of criminal, civil and/or administrative penalties on individuals and/or the Firm.

Background

As part of its day-to-day operations, the Firm and its Affiliates manage investment vehicles in which public entities may invest. These public entities may invest assets that are generally used to fund state and local pension plans, university endowments and other important public programs. Such public assets may be administered and managed by elected officials who are responsible for selecting investment advisers to manage the funds they oversee.

Certain business procedures, often referred to as “pay-to-play” practices, involve investment advisers who seek to do business with state and local governments by making political contributions to those elected officials or candidates who might be able to influence the selection process. Those elected officials who allow political contributions to play a role in the management of these public assets violate the public trust by not only rewarding those investment advisers who make political contributions but also punishing those who do not. As a result, certain laws have been adopted to restrict the ability of investment advisers, and their personnel, from engaging in such political activities. This Policy is intended to both comply with all applicable law and also avoid any outward appearances of impropriety by Firm Employees.

Compliance Officer

It is the Compliance Officer’s responsibility to coordinate the Firm’s adherence to this Policy, and any questions or comments regarding this Policy and the restrictions and procedures should be directed to her (at compliance@500.co).

Specific Restrictions

Effective immediately, and subject to any pre-clearance exceptions, all Employees and Family Members shall comply with the following restrictions (definitions for capitalized terms provided at the end of this Policy):

- Employees and Family Members are prohibited from making any Political Contributions provided, however, that an Employee or a Family Member is permitted to make Political Contributions to state and local government officials or candidates for state/local government office in an aggregate amount not to exceed to $350 per election, per official or candidate, per family, and only for officials and candidates in an election for which such Employee or Family Member was entitled to vote at the time such Political Contributions were made; provided, further, that an Employee or a Family Member is permitted to make Political Contributions to state and local government officials or

candidates for state/local government office in an aggregate amount not to exceed to $150 per election, per official or candidate, per family, and only for officials and candidates in an election for which such Employee or Family Member was *not* entitled to vote at the time such Political Contributions were made. Contributions to federal government officials and candidates that do not constitute Political Contributions (as specifically defined below) are not prohibited by this Policy.

- Employees and Family Members are prohibited from providing or agreeing to provide any payment to a third party (or otherwise hiring or engaging any such third party) to solicit a Government Entity for any services on behalf of the Firm, unless such third party has been confirmed by the Compliance Officer to be a registered broker-dealer or investment adviser that is subject to applicable pay-to-play prohibitions. Examples of such prohibited third parties include, but are not limited to, unregulated persons and entities commonly referred to as placement agents, finders, brokers or consultants.

- Employees and Family Members are prohibited from organizing, coordinating or soliciting any person or entity (to include a political action committee) to make any Political Contribution or any payment to a political party of a state or locality. For the avoidance of doubt, this prohibition includes Political Contributions made through a third party (such as a gatekeeper) or via fundraising events that, in either case, benefit a person or a political party. Note that this prohibition on organizing, coordinating or soliciting applies regardless of whether such Employee or Family Member has made a Contribution.

- Employees and Family Members are prohibited from managing or controlling any political action committee.

Specific Procedures
All Employees and Family Members shall comply with the following procedures:

- Each Political Contribution and each Contribution to a political action committee or political party (regardless of whether such Contribution to the political action committee or political party constitutes a Political Contribution) by an Employee or Family Member shall be reported to the Compliance Officer (at compliance@500.co) and must be pre-cleared by the Compliance Officer prior to being made. In addition, an Employee shall also include in such report all instances of such Employee or associated Family Member organizing, coordinating or soliciting any person or entity (to include a political action committee) to make any Contribution to an official of a Government Entity, to a political party or to a political action committee during such period. All such reports shall be made by the associated Employee and shall include (i) the name of the contributor, (ii) the relationship of such contributor to the Employee, (iii) the amount of such

Contribution (or a description of such Contribution, if such Contribution was not made in cash), (iv) the date such Contribution was made, (v) the name and title (to include any city/county/state or other political subdivision) of the recipient of such Contribution; (vi) a complete description of such organizing, coordinating or soliciting, if applicable; and (vii) any additional information as may be requested by the Compliance Officer.

- Prior to making any Contribution to a political party or a political action committee permitted under this Policy, an Employee and his/her associated Family Member shall use reasonable efforts to obtain written assurances from each permitted political party or political action committee to which they make a Contribution that such political party or political action committee shall not in any event use such contributed funds in any manner that would cause such contributed funds to be a Political Contribution.

- The Compliance Officer shall maintain records containing the information specified above (or such additional information as may be required by applicable law) for all Political Contributions by Employees and Family Members.

- Each potential new Employee must report to the Compliance Officer (at compliance@500.co) all of the Political Contributions made by such potential new Employee and his/her Family Members during the preceding 24 months. Such report shall include the information listed in the first bullet above.

- Employees will report any violations of this Policy to the Compliance Officer (at compliance@500.co), unless the violations implicate the Compliance Officer, in which case such Employee shall report to the Executive Team of the Firm. Such reports will be confidential, and such Employee will suffer no retaliation for making them.

- As soon as practicable after an individual becomes an Employee, the individual shall be required to review this Policy, ask any questions of the Compliance Officer and execute a confirmation. Not less frequently than once during each 12-month period, the Compliance Officer shall provide updated information regarding this Policy to all Employees.

- Each Employee is responsible for ensuring that such Employee's Family Members understand, agree to and abide by this Policy. Any breach of, or non-compliance with, this Policy by a Family Member could result in discipline or dismissal of the associate Employee.

- The Firm shall maintain executed copies of this Policy (in original or electronic form) for not less than six years after termination.

Pre-Clearance Exceptions

On a case-by-case basis, the Compliance Officer may, in his or her sole and absolute discretion, pre-clear any proposed Political Contributions or other activities by an Employee or Family Member that would otherwise be required or not be permitted under this Policy (other than such activities by the Compliance Officer or his or her Family Members, in which case the Chief Executive Officer or Chief Operating Officer of the Firm shall provide such pre-clearance in their sole and absolute discretion). Any such pre-clearance must be approved in advance by the Compliance Officer in writing and specifically name such Employee or associated Family Member. It is anticipated that any pre-clearance exceptions shall be granted, if at all, for exceptional cases in which extenuating circumstances merit such approval.

Political Contributions Outside the United States

Additionally, all Employees are reminded of their obligations under the Foreign Corrupt Practices Act and the Firm's Anti-corruption and Bribery Policy (as set out at page 34) which may apply to any Contributions made for the purpose of influencing any elections for government office outside of the United States. Any concerns or questions relating to political contributions outside of the United States should be addressed to the Firm's Compliance Officer.

Definitions. For purposes of this Policy, the following definitions shall apply:

Contribution means any gift, subscription, loan, advance, payment or deposit of money or anything of value.

Family Member means an Employee's spouse and each member of an Employee's immediate family who lives in the same household as the Employee. For purposes of this Policy, a member of an Employee's immediate family shall include such Employee's parents and grandparents, children and grandchildren, brothers and sisters, mother-in-law and father-in-law, brothers-in-law and sisters-in-law, daughters-in law and sons-in-law, in each case regardless of whether such relationship is by blood, adoption or marriage (e.g., step brothers, step sisters, etc.). For the avoidance of doubt, a member of an Employee's immediate family who does not live in the Employee's household *shall not* be considered a Family Member of such Employee.

Government Entity means any state or any political subdivision of a state of the United States, including (i) any agency, authority or instrumentality of a state or political subdivision; (ii) a plan, program or pool of assets sponsored or established by a state or a political subdivision or any agency, authority or instrumentality thereof; and (iii) officers, agents or employees of a state or political subdivision or any agency, authority or instrumentality thereof, acting in their official capacity.

Political Contribution means any Contribution (whether made directly or indirectly and whether made to a person, a political party or an entity such as a political action committee or otherwise) in the United States for (i) the purpose of influencing any election for state or local office; (ii) the purpose of influencing any election for federal office for the benefit of a candidate who at the time of such election is an official of a Government Entity; (iii) the payment of debt incurred in connection with any such election described in the preceding clauses (i) or (ii); or (iv) transition or inaugural expenses of the successful candidate for state or local office.

Solicit. The term "solicit" means (i) with respect to investment advisory services, to communicate, directly or indirectly, for the purpose of obtaining or retaining a client for, or referring a client to, the Firm or its affiliates; and (ii) with respect to a contribution or payment, to communicate, directly or indirectly, for the purpose of obtaining or arranging a contribution or payment.

Updates
This Policy shall be updated from time to time as circumstances warrant.

Acknowledgement and Agreement
All Employees are required to sign the *Certificate of Acknowledgement and Agreement* attached in Exhibit A and return to the Compliance Officer.

INSIDER TRADING POLICY
December 15, 2021

Summary of Policy Highlights
While it is required that each Employee read this Policy in its entirety, below is a summary of the most important points covered by the Policy.

- Insider trading is illegal, and may be punishable by severe criminal, civil and/or administrative penalties.

- No Employee may trade in any security of any company in violation of any state or federal securities law.

- No employee shall trade in any securities (private or public) where they are in possession of material, nonpublic information related to that company.

- Employees are required to seek the consent of the Compliance Officer for **any** sale or purchase of private company Securities and such investments must comply with the limits set out below.

- Employees may not make personal trades of securities of any "Covered Company" (i.e., any company listed on the Firm's Restricted List from time to time by the Compliance Officer). It is the duty of each Employee to be familiar with companies listed on the Firm's Restricted List and to observe the requirements of this Policy.

- Employees who serve as directors or officers of a portfolio company may be subject to such company's insider trading policy.

- This Policy covers Employees, as well as family members who reside with the Employee and others who live in the Employee's household, as well as entities controlled by such persons.

Policy Statement
It is the unconditional policy of the Firm to comply with all applicable laws and regulations that restrict or regulate investment advisers and their personnel from engaging in the misuse of nonpublic information, to include insider trading and related activities. This Policy is designed to prevent insider trading (or allegations of insider trading) and to protect the Firm from liability for such acts as well as its reputation for integrity and ethical conduct.

This Policy mandates that all Employees refrain from trading on the basis of material, nonpublic information. It is important that Employees understand the breadth of activities that constitute illegal insider trading and the penalties, which can be severe. The consequences of non-compliance with this Policy could result in discipline or dismissal of an Employee, as well as the imposition of criminal, civil and/or administrative penalties on individuals and/or the Firm.

Background
Federal securities laws prohibit any person from buying and selling securities if that person, by virtue of his or her relationship with the company, has access to undisclosed (nonpublic) material information concerning the company. Likewise, these laws prohibit persons who are aware of such material nonpublic information from disclosing this information to others who may trade. The Firm and its controlling persons may also be subject to liability if they fail to take reasonable steps to prevent insider trading by Employees.

Although the Firm itself does not issue securities subject to insider trading prohibitions, it nevertheless has significant exposure to potential insider trading liability. Participation by Employees as directors of portfolio companies and the Firm's knowledge of their activities may expose Employees to inside information from time to time. Employees may also acquire inside information regarding public companies outside the Firm's investment portfolio, as may occur in the course of the acquisition of one of the Firm's private companies by an unrelated public company.

Penalties for Noncompliance

Violations of such laws may be punished by incarceration for a period of up to 20 years, criminal fines of up to $5 million and civil fines of up to three times the profit gained or loss avoided. If the Firm fails to take appropriate steps to prevent illegal insider trading, the Firm may have "controlling person" liability for a trading violation, with civil penalties of up to the greater of $1 million or three times the profit gained or loss avoided, as well as a criminal penalty of up to $25 million. The civil penalties can extend personal liability to the Firm's managers, officers and other supervisory personnel if they fail to take appropriate steps to prevent insider trading.

Failure to comply with this Policy may also subject an Employee to Firm-imposed sanctions, including dismissal, whether or not such Employee's failure to comply with this Policy results in a violation of law.

Compliance Officer

It is the Compliance Officer's responsibility to coordinate the Firm's adherence to this Policy, and any questions or comments regarding this Policy and the restrictions and procedures should be directed to her (at compliance@500.co).

Applicability

This policy specifically applies to all "insiders" (including, but not limited to, Employees and members of their families and others living in their household) who possess, or have access to, material information concerning any company that has not been fully disclosed to the public. Insider trading liability arises when an insider **trades** (a purchase or sale) or **advises others to trade** in securities while in possession of material information concerning the issuer of the securities that has not been fully disclosed to the public.

As noted above, insider-trading proscriptions are not limited to trading by the insider alone; it is also illegal to advise others to trade on the basis of undisclosed material information. An Employee may not pass material, nonpublic information on to others or recommend to others the purchase or sale of any securities when the Employee is aware of such information. This practice, known as "tipping," also violates the securities laws and can result in the same civil and criminal penalties that apply to insider trading, even though an Employee did not trade and

did not gain any benefit from the other person's trading. Liability in such cases can extend both to the "tippee" (the person to whom the insider disclosed inside information) and to the "tipper" (the insider himself).

Special Note on Applicability of the Policy to Digital Assets and Cryptocurrencies

- Generally, personal investments in digital assets and cryptocurrencies are treated as commodities or currencies for regulatory purposes and thus are not subject to the restrictions on investments in private securities described in this Manual.
- However, as this is an emerging industry with developing regulations, Employees should review the following considerations and contact the Compliance Officer if there are any questions on the applicability of this policy:
  - If a token conveys an equity or ownership interest in a company, the token may be considered a security and is subject to the requirements of this policy.
  - If 500 Global has a substantial holding of the token such that 500 Global's decision to sell or buy may reasonably impact the market price, the token may be temporarily added to the Firm's "Restricted" list. Employees may not Trade any tokens included on the "Restricted" list.
  - Investment personnel who have fiduciary duties to a fund and are responsible for investment decisions should contact the Compliance Officer before proceeding to make any personal Trade in tokens that are held by a fund.

Specific Restrictions

- Employees must report any information in their possession which has the potential to be classified as material nonpublic information to the Compliance Officer as soon as possible. Employees should not make a judgment on whether or not they believe specific information to be classified as 'material'. Determination of whether specific information is defined as material nonpublic information is a complex legal determination and should only be undertaken by the Compliance Officer or Firm's General Counsel.

- Employees who know material nonpublic information concerning a company may not Trade or advise others to Trade in that company's securities (even where such Trade is less than the thresholds below). This prohibition applies to family members and others living in the same household as the Employee, as well as entities controlled by such persons.

- Employees, as well as entities controlled by such persons, are prohibited from making a Trade or series of related Trades in the securities of any private company without written pre-clearance from the Firm's Compliance Officer.

- Any Employee Trades in private company securities where the Employee is not in possession of any material nonpublic information concerning a company shall be subject to the following restrictions:
    - **Managing Members & Thematic Fund Managers:** personal Trading in the securities of Private technology companies is prohibited other than in extenuating circumstances (which should be discussed with the Compliance Officer prior to any Trade). In exceptional cases, pre-clearance may be provided - the Compliance Officer shall submit any requests for preclearance to the Chief Executive Officer or the Chief Operating Officer to approve the Trade. Any trades so approved are subject to the same financial limits as all other Employees (no one Trade is in excess of $25,000 and the aggregate value of such Trades within a calendar year (e.g. from January 1 to December 31) do not exceed $100,000);
    - **Part-time Entrepreneurs in Residence ("EIR")**: subject always to pre-clearance with the Compliance Officer and provided such EIR is not involved in making any investment decisions, EIRs are permitted to Trade in private company securities without restriction; and
    - **All other Employees:** subject to pre-clearance with the Compliance Officer, Employees shall be permitted to make an unlimited number of Trades provided no one Trade is in excess of $25,000 and the aggregate value of such Trades within a calendar year (e.g. from January 1 to December 31) do not exceed $100,000.

- Employees and Employees' family members and others living in the same household as an Employee, as well as entities controlled by such persons, are prohibited from making any Trades in the securities of any "Covered Company" (i.e., any company listed on the Firm's "Restricted" list from time to time by the Compliance Officer).

- Employees and Employees' family members and others living in the same household as an Employee, as well as entities controlled by such persons, are prohibited from making a Trade or series of related Trades in the securities of any portfolio investment of any of the Funds, without written pre-clearance from the Firm's Compliance Officer.

- These general prohibitions are subject to the following exceptions:

    - a Trade pursuant to an interest in a pooled investment vehicle, mutual funds, money market accounts and securities managed by a third party investment

manager to whom the Employee or family member have given complete trading discretion; or

- a Trade undertaken by an Employee or an Employee's family member pursuant to their employment or service relationship with an independent third party. In the case of an Employee such relationships held by an Employee must be disclosed and approved by the Compliance Officer in accordance with the Conflicts of Interest policy set out on page 29.

- IMPORTANT NOTE: making a series of smaller Trades in a company each of which is under the thresholds outlined above in order to circumvent the restrictions herein is prohibited and will be treated as intentional misconduct and will be taken extremely seriously by the Firm.

Pre-Clearance Procedures

- Employees (as well as entities controlled by such persons) may not engage in any private company securities Trade in excess of the thresholds set out above without first obtaining the pre-clearance of the transaction from the Compliance Officer.

- A request for preclearance must be submitted to the Compliance Officer at least 24 hours in advance of the proposed transaction using the request form listed on the Compliance team site.

- The Compliance Officer is under no obligation to approve a Trade submitted for preclearance and may determine not to permit the Trade if they are aware that the Firm is in possession of material nonpublic information related to that Company or there is a significant conflict of interest.

- Trades which involve a conflict of interest, such as an Employee investing into a portfolio company may require additional approvals from the Advisory Board of the relevant fund.

- The Compliance Officer should submit any requests for preclearance to the Chief Executive Officer or the Chief Operating Officer to approve the Trade.

Ongoing Responsibilities

- For all approved holdings of private company securities (including both those declared when joining the Firm and those for which pre-clearance was obtained) Employees have an ongoing, affirmative duty to notify the Compliance Officer of any material changes to the holdings, including but not limited to a merger, acquisition, public offering, dissolution or the sale of the interest.

General Cautions

Timing

It does not matter that the "insider" may have decided to engage in a transaction before learning of the undisclosed material information or that delaying the transaction might result in economic loss. It is also irrelevant that publicly disclosed information about a company might, even aside from the undisclosed material information, provide a substantial basis for engaging in the transaction.

Directors and Officers

Employees who are directors or officers of a company, as well as Employees who otherwise have access to inside information on a regular basis (*e.g.*, receipt of monthly financial highlights), should be particularly careful to avoid questionable transactions. Furthermore, Employees who serve as officers or directors of portfolio companies must also comply with the insider trading policies of such companies.

Appearances

Given the hindsight nature of any SEC investigations, avoiding the **appearance** of transacting in a company's stock on the basis of material undisclosed information can be as important as avoiding a transaction **actually** based on such information.

Size of Transaction

There are no limits on the size of a transaction that will trigger insider-trading liability; relatively small trades have in the past occasioned SEC investigations and lawsuits.

Hardships

The existence of a personal financial emergency or hardship does not excuse an Employee from complying with this Policy.

Post-Termination Transactions

To the extent an Employee became aware of material, nonpublic information regarding a company prior to the termination of such Employee's employment or service relationship with the Firm, then this Policy shall continue to apply to such Employee's transactions in the securities of such company until such information has become public or is no longer material.

Fund Opportunities

The Firm's Investment Professionals are reminded that any investment opportunities of $10,000 or more that are made available to them that might reasonably be viewed as an investment opportunity of any of the Funds must be presented to the General Partner of the relevant Fund.

Conflicts of Interest Policy

Additionally, all Employees are reminded of their obligations under the Firm's Conflicts of Interest Policy, as set out at page 29 as such policy relates to personal investments by Employees.

Definitions

Covered Company: means those companies listed on the Firm's "Restricted" list from time to time by the Compliance Officer.

Investment Professional: means Members of the Firm's investment team or any Employees undertaking any investment related activities.

Material Information: It is not possible to define all categories of material information. Determination of materiality is a complex process and should only be undertaken by the Compliance Officer or the Firm's General Counsel. Employees should not make their own judgment on whether information constitutes Material Information **In general, information should be regarded as material if there is a substantial likelihood that a reasonable investor would consider it important in deciding whether to buy, hold or sell a security.** Under this standard, materiality depends upon the particular facts and circumstances of each individual case. However, any information that could reasonably be expected to affect the price of a security is material. Depending on the circumstances, any of the following may constitute material information:

- earnings guidance, including projections of future revenues, costs, earnings or losses, changes to previously announced earnings guidance, or the decision to suspend earnings guidance;
- earnings or operating results that are inconsistent with the consensus expectations of the investment community;
- a pending or proposed merger, acquisition or tender offer or an acquisition or disposition of significant assets;
- a change in executive management or key personnel, a significant pending or proposed joint venture, a company restructuring, or a significant related party transaction;
- major events regarding the company's securities, including a change in dividend policy, the declaration of a stock split, the offering of additional securities or the establishment of a repurchase program;
- bank borrowings or other financing transactions out of the ordinary course;
- severe financial liquidity problems or an impending bankruptcy;
- actual or threatened major litigation, or the resolution of such litigation;
- significant technology events, such as major discoveries or significant developments of or changes in products, research or technologies, including defects or modifications;

- new major contracts, orders, suppliers, customers, partners or finance sources, the loss or deferral thereof or major marketing change;
- the acquisition or licensing of products or product candidates, the introduction or a change in status of significant new products, or a significant change in the company's pricing or cost structure;
- a change in auditors or notification that the auditor's reports may no longer be relied upon;
- the imposition of a ban on trading in a company's Securities; and
- any other factors that would cause a company's financial results to substantially differ from analyst's estimates.

Both positive and negative information can be material. Because trading that receives scrutiny will be evaluated after the fact with the benefit of hindsight, questions concerning the materiality of particular information should be resolved in favor of materiality. In case of doubt, trading should be avoided. If an Employee believes he or she may potentially be in possession of Material Information, he or she should contact the Compliance Officer (at compliance@500.co) for determination.

Nonpublic information: means information that is not generally known or available to the public. One common misconception is that material information loses its "nonpublic" status as soon as a press release is issued disclosing the information. In fact, information is considered to be available to the public only when it has been released broadly to the marketplace (such as by (i) disclosure through the Dow Jones "broad tape" or a newswire service, (ii) broadcast on a widely-available radio or television program, (iii) publication in a widely-available newspaper, magazine or news website, or (iv) filing public disclosure documents with the SEC that are available on the SEC's website) ***and*** the investing public has had time to absorb the information fully. As a general rule, information is considered nonpublic until the close of the second full trading day after the information is released. For example, if a company announces earnings before trading begins on a Tuesday, then the first time an Employee can buy or sell such company securities is the opening of the market on Thursday (assuming the Employee is not aware of other material nonpublic information at that time). However, if the company announces earnings after trading begins on that Tuesday, then the first time an Employee can buy or sell company securities is the opening of the market on Friday.

Securities: The term "securities" includes all stock of a company, such as common stock and preferred stock, as well as derivative instruments, such as options, warrants, puts, calls or other contractual arrangements related to such company's stock.

Trade, Trading: These terms relate to a gift, loan, pledge or hedge, a contribution to a trust, and any other purchase, sale, acquisition, disposition or transfer of securities of a company,

as well as any voluntary exercise, conversion or similar transaction related to the securities of a company.

Updates
This Policy shall be updated from time to time as circumstances warrant.

Acknowledgement and Agreement
All Employees are required to sign the *Certificate of Acknowledgement and Agreement* attached in Exhibit A and return to the Compliance Officer.

INFORMATION SECURITY PROGRAM
December 15, 2021

Purpose
The purpose of this Information Security Program is to comply with all applicable laws and regulations designed to protect the nonpublic personal information (the "***Private Information***") of the Firm's investors, Employees, portfolio companies and service providers with whom the Firm does business (each, a "***Protected Person***"). The specific objective of the Information Security Program is to accomplish the following: (a) to ensure the security and confidentiality of Private Information in a manner consistent with industry standards and as required by applicable state and federal law; (b) to protect against any anticipated threats or hazards to the security or integrity of the Private Information; and (c) to protect against unauthorized access to or use of the Private Information that could result in substantial risk of harm or inconvenience to any Protected Person.

Compliance Officer

It is the Compliance Officer's responsibility to implement, maintain, administer and coordinate the effectiveness of the Information Security Program. Any questions or comments regarding the Information Security Program should be directed to her (at compliance@500.co).

Risk Assessment

As of the adoption of this program, the Firm has identified the following potential internal and external risks to the security, confidentiality and integrity of Private Information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information:

- unauthorized access to documents containing Private Information by Employees (or former Employees), service providers, Protected Persons or third parties, either physically at Firm facilities or electronically through the Firm's information technology system;
- inappropriate use or disclosure of Private Information by Employees (or former Employees), service providers, Protected Persons or third parties who are authorized to have access to Private Information;
- general security risks posed to the Firm's information technology system, including the theft or loss of computers or other equipment permitting access to Private Information, the loss of Private Information due to electrical outages or other computer system failures, and the introduction of viruses into the Firm's information technology system; and
- the loss of documents containing Private Information through unanticipated physical hazards such as fire or floods.

The Compliance Officer shall periodically reassess the reasonably foreseeable internal and external risks to the security, confidentiality and integrity of Private Information. Such assessment will include analysis of, among other things, (i) the effectiveness of Employee training and management with regard to the treatment and handling of Private Information, (ii) the reliability and suitability of the Firm's information technology systems in light of the objectives of this program, including network software design, as well as information processing, storage, transmission and disposal, and (iii) the ability to detect, prevent and respond to attacks, intrusions or other system failures.

Limiting Private Information

The Firm shall use all reasonable efforts to (a) limit the amount of Private Information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected; (b) limit the time such information is retained to that reasonably necessary to accomplish such purpose; and (c) limit access to those persons who are reasonably required to know such

information in order to accomplish such purpose or to comply with state or federal record retention requirements or such other applicable legislation in force from time to time.

Identification of Private Information
The Firm shall use all reasonable efforts to identify paper, electronic and other records, computing systems, and storage media, including laptops and portable devices used to store Private Information, to determine which records contain Private Information.

Risk Management and Control Procedures
Effective immediately, all Employees shall comply with the following procedures to help ensure the security, confidentiality and integrity of Private Information:

Facilities Management.
The Firm shall use commercially reasonable efforts to restrict access to Private Information only to such Employees and service providers who require access in order to perform their designated job functions or services. Where possible and relevant, storage areas containing material Private Information will be reasonably protected against destruction or potential damage. In furtherance of the foregoing, the Firm will impose the following restrictions:

- access to Investor Questionnaires, Limited Partnership Agreements and other records containing Private Information shall be restricted to key personnel as may be approved by the General Partner or the Compliance Officer from time to time;
- documents containing capital account and capital commitment information relating to any Limited Partner shall be stored out of sight of non-personnel;
- all access doors to the Firm's offices shall be locked and only accessible by authorized Employees or other authorized tenants. Employees shall escort their visitors at all times while on site.
- Terminated employees shall be required to surrender all keys, IDs, access codes, badges, business cards, electronic access and the like that permit access to the Firm's premises and/or systems.

Internal Computer Network Controls
The Firm will use commercially reasonable efforts to put reasonable controls in place to restrict access to the Firm's software platforms, programs, files and accounts to only those Employees who require such access to perform their job functions as determined by the Compliance Officer. Such controls will include the following.

- All Employee access to all material programs and networks (such as email or cloud storage platforms) which may contain Private Information shall be subject to secure user authentication protocols which may include: (i) controlled user IDs and other identifiers, which are changed periodically; (ii) reasonably secured

method of assigning and selecting passwords; (iii) restricted access to active users and active user accounts only; and (iv) blocked access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system. .

- Following the termination of employment of any Employee, all necessary steps shall be taken to prevent such terminated Employee from accessing records containing Private Information by, among other things, immediately terminating their physical and electronic access to such records, including deactivating their passwords and usernames.

- Employees shall ensure all sensitive information is transmitted securely and restricted only to relevant personnel.

- Employees shall exercise reasonable commercial efforts to ensure that all material Private Information stored on laptops or other portable devices, (whether personal or provided by the Firm) is stored securely.

External Computer Network Controls

Electronic access to Private Information through the Firm's website or investor relations portal, or otherwise, shall be restricted to: (i) the Protected Person whose Private Information is contained therein; (ii) other Protected Persons, to the extent that such access is permitted pursuant to the governing organizational document or other applicable contract and applicable law; and (iii) the Firm's Employees and service providers who require access in order to perform their designated job functions or services. Such controls will include the following:

- access to any portion of the website or investor relations portal containing Private Information shall be password protected;
- critical data stored on the website or investor relations portal, including Private Information, shall be backed up on a regular basis by the relevant external provider; and
- the ability to publish information on the website or modify existing information contained thereon shall be restricted to the relevant personnel as may be approved by the relevant General Partner or the Compliance Officer from time to time.

Service Providers

Prior to engaging any third-party service provider who may receive Private Information, the Firm will take commercially reasonable measures to determine whether such service provider maintains sufficient procedures to detect and respond to security breaches, as required by this Information Security Program and applicable law. If necessary, the Firm may require a prospective service provider to certify to it that it maintains such procedures. Contracts with

service providers will contain commercially appropriate provisions to protect the security, confidentiality and integrity of all Private Information that is in their possession. The Firm will undertake to monitor the Firm's service providers' compliance with such contractual provisions as well as the service provider's own internal security procedures on a case-by-case basis depending on the sensitivity of any relevant Private Information in their possession.

Employee Management and Training

The Firm shall implement appropriate measures to ensure that all Employees are informed of and comply with the Information Security Program including the following measures.

- The Human Resources team or other individual responsible for hiring shall check the references and background (if applicable) of any prospective Employees who may have access to Private Information.

- The Compliance Officer will be available to discuss the Information Security Program with all Employees, each of whom shall execute a copy hereof. Each Employee hired by the Firm following adoption of the Information Security Program shall also be required to read and execute a copy of the Information Security Program.

- The Firm's Employees shall be trained to take basic steps to maintain the security, confidentiality and integrity of Private Information, which may include topics such as: securing and restricting access to material Private Information; using password-activated screensavers; using strong passwords; periodically changing passwords; disposing of Private Information in a secure manner; not keeping open files containing Private Information on their desks when they are not at their desks; and securing all physical and electronic files at the end of the work day in a manner consistent with this Information Security Program.

- The Firm will impose disciplinary measures for any breaches of the Information Security Program by Employees. Such measures could include: a letter of censure, a suspension (with or without pay), a fine, a demotion, termination of officership or termination of employment. In determining what action is appropriate in a particular case, the Firm will take into account all relevant information, including the nature and severity of the violation, whether the violation was a single occurrence or repeated occurrences, whether the violation appears to have been intentional or inadvertent, whether the individual in question had been advised prior to the violation as to the proper course of action and whether or not the individual in question had committed other violations in the past.

- Employees are encouraged to report to the Compliance Officer (at compliance@500.co) any suspicious or unauthorized use of Private Information.

Breaches of Security

Employees shall notify the Compliance Officer immediately upon becoming aware of any unauthorized disclosures or breaches of security. The Compliance Officer shall conduct a mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of Private Information following any incident involving a breach of security. The Compliance Officer shall document the foregoing and provide a report to the General Partner of any affected Fund.

Employees should notify the Human Resources department immediately upon the loss or theft of any laptops or other devices (whether personal or provided by the Firm) which may contain any Private Information.

Routine Testing of Controls, Systems and Procedures

The effectiveness of the Information Security Program will be regularly evaluated and tested through the use of commercially reasonable audits and operational testing where appropriate. Where possible and appropriate, security procedures will be tested and verified regularly The Firm shall use commercially reasonable efforts to monitor its systems, for unauthorized use of or access to personal information.

Security Program Evaluation and Adjustment

The Compliance Officer will regularly monitor, evaluate and adjust the Information Security Program in light of the Firm's activities and the results of any testing and monitoring of the program. The Compliance Officer shall review the Information Security Program at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing Private Information to ensure that it is reasonably consistent with industry standards and applicable law, and contains administrative, technical, and physical safeguards to sufficiently ensure the security and confidentiality of the Private Information. In connection with such review, the Compliance Officer will evaluate and adjust the Information Security Program as appropriate to address: (i) the current risk assessment, management and control activities; (ii) any new risks or vulnerabilities identified by the Compliance Officer using the standards set forth above; (iii) any technology changes that may affect the protection of Private Information; (iv) material changes to the Firm's business, including to the size, scope and type of the Firm's business; (v) the amount of resources available to the firm; (vii) the amount of Private Information stored or held by the Firm; (viii) any increased need for security and confidentiality of both investor and employee information; and (ix) any other circumstances that the Compliance Officer believes may have a material impact on the Information Security Program. The Compliance Officer will provide the Firm's management with regular reports on the status of the Information Security Program, compliance

problems (if any) relating thereto and recommendations for improvement thereof. The Compliance Officer will also provide updated information regarding the Information Security Program to all Employees.

Executed copies of these policies and procedures shall be retained (in original or electronic form) for not less than six years.

CONFLICTS OF INTEREST POLICY
December 15, 2021

Policy Statement
It is the policy of the Firm, to proactively identify, monitor, disclose and manage any conflicts of interest that may arise during the course of business to ensure that they do not adversely affect the Firm or the Firm's investors.

The Firm and its Employees may owe legal duties of loyalty and trust towards the Firm's investors. When such duties apply, the Firm, and the Funds it manages must put the interests of their investors above their own interests and must not profit from their responsibilities except with the knowledge and consent of the investor.

Compliance Officer
It is the Compliance Officer's responsibility to coordinate the Firm's adherence to this Policy, and any questions or comments regarding this Policy and the restrictions and procedures should be directed to her (at compliance@500.co).

Identification of potential conflicts of interest
A conflict of interest may arise, in any area of the Firm's business, where the Firm or any of its Employees:

- has an interest (personal or professional) that conflicts with the interests of any of the Firm's clients or investors, including a conflict that may arise within the Firm itself (e.g., in the context of a fund manager, having economic interest in or receiving other pecuniary incentives from an 'Ecosystems' contract while still actively managing a Fund);
- is likely to make a financial gain (or avoid a loss) at the expense of any of the Funds or investors;
- is interested in the outcome of the service provided to a Fund or investor where the Firm's interests are distinct from investor interests;
- has a financial or other incentive to favor the interests of one Fund or investor over another; or
- receives money, goods or services from a third party in relation to services provided to the Firm, its Affiliates (including the Funds) or investors other than standard fees or commissions.

The Firm has taken reasonable steps to identify conflicts of interest that exist, or may exist:

- between the Firm and its investors;
- between one investor and another; and
- between the Funds it advises.

In the context of the Firm's business activities, the most common potential conflicts of interest identified include potential conflicts of interest:

- between the personal interests of the Firm's Employees and the Funds advised by the Firm;
- arising from the discretionary allocation of suitable investment opportunities, co-investment opportunities and fees and expenses across the Funds advised by the Firm;
- arising from the receipt of revenue for the provision of services from one of the Funds' portfolio companies;
- arising from the appointment of Affiliates or portfolio companies to provide services to the Funds or the Firm for compensation;
- arising from the appointment of service providers by the Firm or its Affiliates in which an Employee has a personal interest; and
- arising from the receipt of revenue, profit or commission for the provision of certain 'Ecosystem' consulting or investment advisory services by the Firm's Affiliates.

There is no strict definition of "conflict of interest" or "personal interest" and it will depend on the circumstances in each case. If in doubt Employees should always err on the side of caution and disclose details of the situation to the Compliance Officer. For the avoidance of doubt, a conflict of interest that arises intra-Firm (i.e., within the context of the Firm and its affiliates' business, and therefore occurring fully within 500 Global such as between a Thematic Fund and the Firm's Ecosystem activities) should still be declared and each individual concerned is responsible for submitting their own disclosures.

Disclosure of potential conflicts of interest

All Employees must disclose in writing to the Compliance Officer all potential conflicts of interest, including those in which they have been inadvertently placed due to either business or personal relationships. Such disclosures should include details of any (i) personal investments; (ii) director, officer or trustee positions; (iii) advisory relationships; and (iv) any other material information that may reasonably give rise to a potential conflict of interest.

This includes family members, business partners, suppliers, business associates or competitors of the Firm. While these guidelines do not intend to interfere with the personal lives of the Firm's Employees, it requires those persons to recognize situations where conflicts of interest may arise and to avoid them when possible.

All Firm Employees undertake to provide full, true and accurate disclosure of any potential conflicts of interest at the time of joining the Firm and to provide immediate notice of any changes thereto to the Compliance Officer. Any such disclosures can be made to the Compliance Officer using the Disclosure of Conflict of Interest form available on the Compliance team site.

Any failure to disclose potential conflicts of interest, whether willful or negligent, will be taken seriously by the Firm. Failure to comply with this Policy may also subject an individual to Firm-imposed sanctions, including dismissal, whether or not such Employee's failure to comply with this Policy results in a violation of law.

Outside Employment and Activities

In line with the Firm's employment policies as effective and disseminated to the Employees from time to time, Employees may undertake additional outside employment, including self-employment, commercial or business ventures, advisory relationships and employment with non-portfolio companies, or may serve as a director or trustee of another for-profit company, subject to the prior written approval of: (i) the Compliance Officer; and (ii) their Manager.

The intention of this policy is to ensure that any additional commitments do not distract from your role at the Firm and that the Firm is able to properly identify any conflicts of interest and if required take any appropriate actions such as disclosing to the relevant advisory board. While the Firm retains discretion to reject any such request, the Compliance Officer generally would only do so in circumstances where the request would pose a significant conflict of interest.

Employees should not undertake paid (including grant of options or advisory shares) advisory work for any of the Firm's portfolio companies.

Employees also are asked to notify the Firm's Compliance Officer if they serve as directors or trustees of governmental or not-for-profit organizations. Any such consent can be made to the Compliance Officer using the Consent to accept Advisory Engagement form available on the Compliance team site.

With regard to any speaking engagement where an Employee is representing the Firm (or disclosing the Employee's association with the Firm):

- Such engagement shall be accepted by Employees only (i) upon invitation, (ii) towards furthering the business goals of the Firm, and (iii) following disclosure by the Employee of such speaking engagement to the Employee's manager; and
- Employees shall not accept any speaking fee or honorarium. In cases where such fee or honorarium is unavoidable, Employees shall transfer such fees to the Firm in full, which amounts the Firm will collate and donate to charity on an annual basis (and specifics of such donations shall be shared with the Employee).

Please discuss with the Compliance Officer or HR Department if any such circumstances apply to you.

Subject to the prior approval of the Compliance Officer and Legal Department, Employees are permitted to run Angellist syndicates offering interests in 500 portfolio companies in a personal capacity provided that the benefit of any carried interest from such syndicate is paid to the Firm or the relevant Fund (as determined with the Legal Team on a case by case basis). If the syndicate relates to a non-portfolio company please discuss with the Compliance Officer.

Employees may not solicit business for themselves or others if it is business in which the Firm or any of the Funds is involved or which they know the Firm or Fund (as relevant) has an interest in developing.

Any part time employees or contractors concerned with any potential conflicts of interest arising from their activities outside the Firm should discuss such activities with the Compliance Officer to identify whether any potential conflicts of interest may arise.

Personal Investments

In accordance with the Firm's Insider Trading Policy (as set out at page 15), Employees must seek prior consent from the Compliance Officer before making any personal investments in private tech companies.

Investment Professionals

Members of the Firm's investment team or any Employees undertaking any investment related activities ("**Investment Professionals**") are reminded that any investment opportunities of $10,000 or more that are made available to them that might reasonably be viewed as an investment opportunity of any of the Funds should be presented to the General Partner of the relevant Fund.

The Firm's Investment Professionals shall be prohibited from making investment recommendations that relate to any securities or companies in which that Investment Professional has an interest, without disclosing their personal interest. Where such an interest exists, the relevant Investment Professional shall remove themselves entirely from any decision-making processes and shall not participate in any investment decisions related to that company.

Any Investment Professional concerned or unclear about whether they would be deemed to have a personal interest in a matter should err on the side of caution and disclose the matter to the Compliance Officer.

Advisory Board Approval

Note, in certain situations, in addition to approval of any potential conflicts of interest by the Compliance Officer, the Firm may also be required to seek consent of the limited partner Advisory Board of the relevant Fund. Employees should note that these are independent committees and the Firm cannot control the outcome of any such submissions for approval.

Certain members of senior management may also be required to seek approval of the Board of Officers of 500 Mothership GP, L.L.C. for certain matters contemplated herein. If you have any concerns or questions in this regard please direct them to the Compliance Officer.

Updates

This Policy shall be updated from time to time as circumstances warrant.

Acknowledgement and Agreement

All Employees are required to sign the *Certificate of Acknowledgement and Agreement* attached in Exhibit A and return to the Compliance Officer.

ANTI-CORRUPTION AND BRIBERY POLICY

December 15, 2021

Policy Statement

The Firm takes a zero-tolerance approach to bribery and corruption. The Firm is committed to acting professionally, fairly and with integrity at all times. Accordingly the Firm expressly prohibits any Employee, when acting on behalf of the Firm or its Affiliates, from accepting, soliciting, paying, offering or promising to pay, or authorize any payment, public or private, in order to secure any improper benefit for themselves or for the Firm or its Affiliates.

Compliance Officer

It is the Compliance Officer's responsibility to coordinate the Firm's adherence to this Policy, and any questions or comments regarding this Policy and the restrictions and procedures should be directed to her (at compliance@500.co).

Giving and Acceptance of Gifts and Entertainment

Firm Employees may not give excessive gifts, items of value, or benefits to any an officer, director, employee, agent or attorney of a financial institution or to a foreign official as described in this policy without prior written approval of the Compliance Officer.

The Firm acknowledges that in some circumstances it may be customary to provide reasonable gifts as tokens of esteem or gratitude, however such gifts may be given only where approved by management or within such limits for the applicable jurisdiction as may be circulated by the Compliance Officer from time to time. Any such gifts must be made openly and transparently and should be properly recorded in the Firm's books and records.

Similarly Employees are permitted to provide reasonable hospitality and entertainment to the Firm's business partners and (non-Government) investors provided that these are legitimate, bona fide expenditures that are either directly related to: (a) the promotion or explanation of the Firm's services; or (b) the execution or performance of a contract with a foreign government or agency thereof. Again, the Firm urges employees to use their best judgment with regard to what is reasonable or appropriate in the circumstances.

If an Employee is unsure about a whether the provision of a proposed gift or any potential hospitality to be to any person or company outside the Firm which is involved directly or indirectly in the business or affairs at the Firm, or is a potential client or investor in the Funds they should seek the prior consent of the Compliance Officer using the form available on the Compliance team site.

All Employees are reminded of the Firm's policies and procedures regarding the acceptance of gifts from outside parties. Employees should not solicit gifts from any party with whom the Firm conducts or could conduct business. Any gift received by an Employee from any third party with

whom we conduct or could conduct business should be reasonable and appropriate in the circumstances.

If an Employee believes that they have received an excessive gift, they should report details to the Compliance Officer. The Compliance Officer may require the return of the gift if the Compliance Officer determines, in their sole discretion, that the gift could improperly influence the use of a third-party service provider or create the appearance of a conflict of interest. This policy does not prohibit Firm Employees from accepting token branded gifts, occasional meal or reception invitations, tickets to a sporting event or theater, or comparable entertainment, that is not so frequent, costly or expensive as to raise any question of impropriety.

Under no circumstances should any Employee solicit these items or other favors in any manner that could be construed as using employment with the Firm to obtain a personal benefit. If an Employee has a question concerning a particular situation, it should be addressed to the Compliance Officer.

IN NO EVENT SHOULD ANY EMPLOYEE ALLOCATE ANY BUSINESS TO A THIRD PARTY ON THE BASIS OF PERSONAL GIFTS OR REWARDS PROVIDED TO THE EMPLOYEE OR A RELATIVE OR FRIEND OF THE EMPLOYEE.

Rebating of Firm Compensation

No team member should rebate, directly or indirectly, to any person or entity any part of the compensation received from the Firm as an Employee.

Questionable Payments

It is a criminal offense for any team member to use the Firm's resources, or make payments of any kind, for the benefit of any government, government official, financial institution[1] or employee thereof, or industry official with the intent of inducing or influencing the recipient to misuse his or her position. Any such action is **forbidden**.

The use of Firm funds or property for any purpose which would be in violation of any applicable law or regulation or would otherwise be improper or give the appearance of impropriety is strictly prohibited. No payments, including amounts paid for entertainment, shall be made to, or for the benefit of, employees of any governmental body, administrative agency, exchange or self-regulatory organization for the purpose of, or in connection with, obtaining favorable actions by such employee, body, agency, exchange or organization. Similarly, Employees are prohibited from giving gifts to government, exchange or self-regulatory employees for any reason.

[1] A "financial institution" includes (1) a bank holding company, (2) a savings and loan holding company, (3) any bank or other institution the deposits of which are insured by the Federal Deposit Insurance Corporation, (4) any member of the Federal Home Loan Bank System, (5) any Federal Home Loan Bank, (6) any credit union the accounts of which are insured by the National Credit Union Share Insurance Fund, (7) any federal land bank, federal land bank association, Federal intermediate credit bank, production credit association and bank for cooperatives and (8) a small business investment company.

No payment on behalf of the Firm shall be approved or made with the intention or understanding that any part of such payment is to be used for any purpose other than that prescribed by the documents supporting such payment. It is strictly prohibited for any person, directly or indirectly, to offer to make any bribes, kickbacks, rebates or other payments to any company, financial institution, person or governmental official to obtain favorable treatment in receiving or maintaining business. No payments or deposits pursuant to any commitment made to any company with which the Firm has business dealings shall be made to any individual or to bank accounts in the names of any individuals.

Financial Institutions Bribery Statute

It is a *felony* under federal law to give, offer or promise an officer, director, employee, agent or attorney of a financial institution (as described in footnote 1 above) *anything* of value in connection with any transaction or business of such financial institution. It is also a federal crime for an officer, director, employee, agent or attorney of a financial institution to solicit or demand (for his or her benefit or the benefit of another person or entity), accept or agree to accept anything of value from any person with the intent to be influenced in connection with any business or transaction of such financial institution. The phrase "anything of value" is comprehensive and expansive and can include literally anything, big or small, tangible or intangible, including ordinary and customary business gifts, drinks, dinners, cab fare, flowers, use of telephones or automobiles, etc. Even for minimal gifts, offers, promises and payments of less than $100, violators face penalties of up to $1,000 and *imprisonment* for up to one year.

It is the Firm's policy that *nothing* of value passes from the Firm or its Employees to *any* employee or agent of a financial institution (as described in footnote 1). *Any violation of this policy, no matter how small, will be considered extremely serious and will result in sanctions, including the possibility of suspension and/or discharge from the Firm*.

Foreign Corrupt Practices Act

General

The Foreign Corrupt Practices Act ("**FCPA**") prohibits making or offering payments to a foreign official in order to obtain or retain business. The terms of the FCPA are interpreted broadly by the two agencies that enforce the law, the US Department of Justice and the SEC. Under threat of significant monetary penalties and imprisonment, the FCPA prohibits any officer, agent or Employee of the Firm from:

- directly or indirectly paying or giving, offering or promising to pay, or authorizing or approving such offer or payment;
- any funds, gifts, services or anything else of any value, no matter how small, or seemingly insignificant;
- to any foreign official or other person specified below (each, a "**Covered Person**");
- for the purpose of obtaining or retaining business, favorable treatment, or other commercial benefits, whether by (i) influencing any act or decision of the Covered Person in his official capacity; (ii) inducing the Covered Person to do or not do

any act in violation of his lawful duty; or (iii) inducing the Covered Person to use his influence to that end with a foreign government or instrumentality;

- while knowing or having reason to know that all or a portion of the funds or items of value will directly or indirectly be forwarded to a Covered Person for such purpose. (Note: "having reason to know" is willfully avoiding or disregarding facts, hints or clues.)

Payments need not be consummated in order to violate the FCPA. Offers and promises to pay are also violations.

Payments need not be made directly to a foreign official. Payments made indirectly through third-party representatives or consultants may be FCPA violations if the Firm or Employee knew or had reason to know that a payment would make its way to a government official.

Who Is A Covered Person?

A "Covered Person" for this purpose is any foreign official including, without limitation, any officer or employee of any foreign government or any governmental department, agency or instrumentality (e.g., a central bank) or any government-owned or controlled enterprise or any person acting in an official capacity for or on behalf of any such government, department, agency, instrumentality or enterprise). It also includes any foreign political party, party official or candidate for political office. Immediate family members of a Covered Person may also be considered covered "officials" under the FCPA. Any doubts about whether a particular person is a government official should be resolved by assuming that the individual involved is a government official for FCPA purposes.

What Is Foreign?

Foreign for this purpose means outside the United States.

Exemptions

There are certain exemptions to the broad prohibitions set forth above. However, these exemptions are very precise and must be discussed with counsel before they can be invoked. No Employee is to discuss or consider any proscribed activity outlined above without the prior approval of the Compliance Officer.

Money Laundering and Proceeds of Crime

What is Money Laundering?

Money laundering is the process by which the illegal nature of criminal proceeds is disguised in order to give a legitimate appearance to such proceeds. Criminals may try to use the Firm to facilitate money laundering by investing the proceeds of crime in the Funds in order to disguise the origins of the money. The Firm is subject to certain legal obligations to prevent money laundering and terrorist financing and all Employees also bear responsibility for compliance with these.

Prevention of Money Laundering

All Employees are required to adhere to these standards to protect the Firm and its reputation from being misused for money laundering and/or terrorist financing or other illegal purposes.

All Employees are expected to conduct appropriate diligence on any potential investors and the source of the funds in question. Employees should refuse to negotiate with or to close an investor if an Employee cannot form a reasonable belief that it knows the true identity of the investor and/or ultimate beneficial owners and the source of any funds they are proposing to invest. In particular Employees should be wary of potential investors willing to invest without reviewing any legal documentation or terms of investment in detail or where an Employee is dealing with an intermediary but the identity of the ultimate beneficial owner is unclear.

The Firm will not accept investments that involve funds that are known or suspected to be the proceeds of criminal activity nor enter into or maintain business relationships with any individuals or entities known or suspected to be a terrorist or a criminal organization or member of such or listed on sanction lists.

Employees are required to comply with the Firm's anti-money laundering policies and LP onboarding processes in place from time to time. Employees should note these may vary from region to region and Employees should discuss the relevant "know your customer" requirements in their specific circumstances with the Compliance Officer or a member of the Legal Team.

Cayman Islands Regulations

All fund investment and fundraising teams should comply with Cayman Islands anti-money laundering and Know-Your-Client requirements, as may be applicable to such teams under the jurisdiction of formation of the funds advised. Please review our Cayman Islands AML/CFT Policies and Procedures Manual and contact the Compliance Officer with any questions on the scope of such rules or actions pending. The purpose of this Manual is to set out Cayman Islands specific Anti-Money Laundering ('AML') / Counter Terrorist Financing ('CTF') / Anti-proliferation Financing ('APF') requirements applicable to each of our entities registered in the Cayman Islands. Such regulations include (1) the Proceeds of Crime Law ("POCL") which creates criminal liability for failure to comply with AML requirements, as described in the POCL, the Money Laundering Regulations ("AMLRs") and Guidance Notes; (2) the Terrorism Law, which criminalizes offences pertaining to terrorism; (3) the Anti-Corruption Law ("ACL") and UK Bribery Act, which address bribery of public oficials, and (4) other Sanctions and Monetary Authority Laws. These regulations require strict compliance with record-keeping, client due diligence and verification procedures prior to establishing business relationships, as well as ongoing monitoring, training and reporting procedures.

Duty to report suspicions

Any Employees with any suspicions about a potential or current investor, or the source of any monies invested or proposed to be invested in the Funds have a duty to report such suspicions to the Compliance Officer in a timely fashion.

Updates

This Policy shall be updated from time to time as circumstances warrant.

Acknowledgement and Agreement

All Employees are required to sign the *Certificate of Acknowledgement and Agreement* attached in Exhibit A and return to the Compliance Officer.

COMMUNICATION AND FUND MARKETING POLICY

December 15, 2021

Policy Statement

The Firm is eager to maintain a good reputation in the market for accurate and timely communication with investors and stakeholders.

Compliance Officer

It is the Compliance Officer's responsibility to coordinate the Firm's adherence to this Policy (which includes the Firm's Docsend Policy), and any questions or comments regarding this Policy and the restrictions and procedures should be directed to her (at compliance@500.co).

Communications with Investors and the Public

Promotional Materials.

The Firm has adopted specific written procedures relating to the origination and distribution of all "Promotional Materials", which include:

- any standardized written presentation, text or material concerning the Firm, the Funds or their businesses;
- any communication of material used for media publication or other dissemination; and
- any standardized reports, letters or other materials used for the solicitation of business.

All written promotional or solicitation material must be approved by the Firm's Legal Department, in writing before its use or dissemination. Pre-approved template marketing materials are available from the Legal Team.

No written promotional or solicitation material should be sent to prospective investors directly via email. Access to all such materials is only permitted to be sent via Docsend to enable the Firm to maintain accurate records. Employees are required to comply with the Firm's Docsend Policy at all times (which is included within and provided at the end of this Communication and Fund Marketing Policy). Employees should direct any questions about distribution of marketing materials via Docsend to the Compliance Officer or a member of the Legal Team.

Use of promotional material mentioning the Firm by third parties should be reviewed and approved by the Legal Department. Please also take note of the guidelines on usage of Social Media and Blog Sites on page 43 below.

Any questions concerning the Firm's promotional activities or policies should be directed to the Compliance Officer. Further information around marketing and investor relations can be found on the Fundraising team site.

The Firm expects any Employees involved in marketing any of the Funds to understand the relevant legal and regulatory restrictions that apply to them. It is the Employee's responsibility to

educate themselves with regard to any applicable domestic and international fundraising restrictions. Employees should ask the Legal Department to make the necessary introductions to local lawyers in the relevant jurisdictions on their behalf if applicable.

General Solicitation and Advertising

At present, the Funds offer interests to investors without registering them under the Securities Act of 1933 ("**Securities Act**") by relying on an exemption under Section 4(2)(a), Regulation D or Regulation S under the Securities Act, which provides an exemption from registration as long as certain conditions are met.

The benefit of relying on Section 506(c) is that the Firm is permitted to generally solicit and market the Funds to investors in the United States e.g. we are permitted to offer or sell Fund interests through:

- advertisements, articles, notices or other communications published in any newspaper, magazine or similar media or broadcast over television or radio; or
- seminars or meetings whose attendees have been invited by any general solicitation or general advertising.

Employees should not publish, share or comment on the existence of any Fund publicly (including on social media) without first seeking approval to do so from the Marketing and Legal Departments, regardless of whether such stories are already being reported by the press.

It is a condition of 506(c) that the Firm take active steps to verify that any investors are "Accredited Investors" (per the third party service provider 'Verify Investor' that the Firm uses).

Note, neither the Firm nor the Funds have as at the date hereof, made any equivalent filings outside the United States and as such the Funds should not be marketed to the general public outside the United States. Note, the Firm is prohibited from actively marketing the Funds in certain geographies (e.g. Europe). Employees with investor interest in such geographies should discuss the matter with the Legal Department prior to commencing any marketing activities for a fund in those geographies.

Aside from potentially severe regulatory and criminal penalties both for the Firm and individual Employees, there are also major civil risks of non-compliance. Failure to comply with local fundraising restrictions may also invalidate an investor's admission to the Fund. Note that in many countries the cost and administrative burden of compliance is significant.

Placement Agents

Use of placement agents, brokers, or other similar third-party facilitators to market or solicit investment in a fund is strictly prohibited, unless prior approval is obtained from the Compliance Officer and appropriate disclosure is included in the relevant fund documents by the Legal team.

Accuracy in Marketing and Investor Due Diligence

Any statement, whether oral or written, that an Employee provides to anyone who may be considering an investment into any of the Funds may be deemed to be "marketing" and an investor may rely on such statements in making a decision to invest in the Fund. If such statements should be deemed to be false or misleading (whether willfully or as the result of an innocent mistake or carelessness) the Firm and any Employees involved may be subject to very serious criminal and civil penalties. In certain circumstances Employees may be held personally liable for such statements.

It is the Firm's policy that Employees are responsible for ensuring that:

- any statements made to the public or potential investors are 100% accurate;
- any factual statements provided in writing (in any marketing documents, presentations, diagrams, email or during the course of due diligence enquiries) must be capable of independent verification and an independent source listed;
- they do not disclose any proprietary or confidential information (such as investor details or portfolio company financial or valuation numbers) without the prior written consent of the investor or company to do so;
- they keep thorough, accurate written records of all conversations and dealings with potential investors. Such records shall be provided to the Compliance Officer on request.

Investor Complaints

All investor complaints, whether written or oral, must be reported to the Compliance Officer immediately upon receipt. If a complaint is in writing, a copy of the complaint must be forwarded to the Compliance Officer. The original written complaint or a written description of an oral complaint must be maintained in a designated file, along with a statement of the details of how the complaint was resolved.

All records relating to resolved investor complaints will be retained in a designated location and must be readily available for review by a regulatory or self-regulatory authority upon request. Any request by a regulatory or self-regulatory authority to see a file related to an investor complaint should be directed to the Compliance Officer.

Communications with the Press

As outlined above, the Firm is permitted to generally solicit and advertise the Funds in the United States. However, Employees should not discuss the existence of any Funds with journalists unless they have the prior approval of Legal and Marketing Teams.

EMPLOYEES SHOULD NOT SPEAK TO ANY JOURNALISTS, RESPOND TO ENQUIRIES FROM JOURNALISTS OR CONFIRM ANY FACTS TO JOURNALISTS WITHOUT THE PRIOR APPROVAL OF THE MARKETING AND LEGAL DEPARTMENTS. IF APPROACHED BY A JOURNALIST FOR COMMENT, PLEASE DIRECT THEM TO PRESS@500.CO UNLESS OTHERWISE INDICATED BY THE MARKETING TEAM.

Avoidance of Rumors

The Firm is committed to helping maintain fair and orderly markets and is aware of the effects that spreading information might have on the prices of securities. Therefore, the Firm and its Employees must avoid the spreading of rumors. Used in this policy, “rumor” means a story or information that is either false or uncertain and is passed among persons. Rumors can be passed along in face-to-face meetings, on the telephone, by email or instant messaging, or posted in Internet chat-rooms or privately maintained websites. The term “rumor” does not normally include information or stories passed on by a reputable public news source like Bloomberg or Reuters, or information publicly disseminated by the government or its officials.

Intentionally originating or spreading a rumor known to be false to manipulate the price of a security is illegal. No Employee shall originate or circulate in any manner a rumor that the Employee knows or has reasonable grounds to believe is false.

The Firm and its Employees are absolutely forbidden from spreading any false rumor that might affect a security’s price.

The Firm and its Employees must use good judgment in disseminating information of uncertain value. In addition, the Firm and its Employees shall not profit by spreading uncertain rumors, and they must also avoid actions that appear to create profits by rumor spreading. In particular Employees should be careful with regard to ‘sharing’ information on social media sites.

Care should always be observed when disseminating non-public information. Even true information may affect a stock’s price, perhaps in a way that cannot be foreseen in advance.

Should there be a legitimate business reason for discussing a rumor within or outside the Firm (e.g., seeking an explanation for an erratic share price movement that could be explained by the rumor), the information must be communicated in a manner that:

1. makes clear that the information is a rumor; and

2. makes clear that the information has not been verified.

Any Employee who has questions about whether a communication is proper should check with the Compliance Officer before sending or otherwise communicating it.

Firm Website and Social Media Pages

Firm websites and social media pages are required to be disclosed on the Firm's Form ADV filing with the SEC. Employees are reminded that all Firm websites and social media pages remain the property of the Firm.

Employees must comply with the Firm's Website and Social Media guidelines in place from time to time. Any questions related to the suitability of content to be published on Firm websites or social media accounts should be referred to Legal or Marketing Teams. An overview of key points to remember are below:

- all Firm microsites (including any thematic fund sites) must display the latest "About Us" global statistics (Marketing can provide this if you are not sure);
- websites must be updated alongside fund marketing materials every quarter to ensure up to date information is displayed;
- any new changes to any Firm website must be approved by Legal;
- notify IT and Legal before creating any new websites;
- branding must be consistent across 500 websites in line with 500 Global branding guidelines (Marketing can provide this if you are not sure);
- respect confidentiality restrictions, never post any:
    - portfolio company valuation, acquisition or financing terms;
    - investor names or identities or information; or
    - Other client / partner names or logos;

  without the prior written approval of the company / investor / partner and Legal.
- do not use any Firm websites or social media channels to advertise or solicit fund investments, if unsure about what is permitted please discuss with the Compliance Officer or Legal;
- do not post Firm news that has not been made public, if you are not sure, please confirm with Legal or Marketing;
- respect financial disclosure laws, in line with the Firm's Insider Trading policy above, it is illegal to communicate or give a "tip" on inside information to others;
- do not "share" news stories around new Funds on social media unless the Marketing and Legal Departments have confirmed it is ok to do so;
- be wary of inadvertently "sharing" information on social media that could be conceived as fund marketing materials without discussing with Legal first; and
- always be honest and accurate.

Employee Personal Social Media and Blog Sites

The Firm understands that social media is integral to modern life and a fun way for Employees to share their life and opinions with family, friends and co-workers around the world. However, the use of social media may also present certain risks and carries with it certain responsibilities.

In general, the Firm requires Employees to exercise discretion and to be careful of making inappropriate comments about the Firm, its Affiliates, Employees, management and/or investors on blogs, Facebook, Twitter, YouTube and other social media outlets. Remember that you may be perceived as representing the Firm when you share certain information and by virtue of your position at the Firm, your innocent posting may been seen to confirm rumored information. Employees should post only appropriate and respectful content remembering these basic guidelines:

- always be honest and accurate;
- maintain the confidentiality of the Firm and its Affiliates' trade secrets and private or confidential information. Employees should not share any details of portfolio company valuations or funding events without prior written permission to do so. Employees should never share any sensitive investor information;
- respect financial disclosure laws, it is illegal to communicate or give a "tip" on inside information to others;
- express only personal opinions; Employees should never represent themselves as a spokesperson for the Firm. If Employees do publish personal blogs or post online related to their work or subjects associated with the Firm, they should make it clear that they are not speaking on behalf of the Firm. It is best to include a disclaimer such as "The postings on this site are my own and do not necessarily reflect the views of 500 Global";
- do not "share" news stories around new Funds unless the Marketing and Legal Departments have confirmed it is ok to do so;
- only share information about the Firm's portfolio company or investors where we have their permission to do so;
- be wary of inadvertently sharing information that could be conceived as fund marketing materials without discussing with Legal first;
- always comply with all requirements of this Manual (including data security and privacy procedures and policies for the prevention of insider trading); and
- Employees should not share content on personal social media channels engaging in what could be misconstrued by the public as inappropriate behavior while wearing or displaying the 500 brand or referencing the Firm in any way (examples include contravening the Firm's policies around consumption of drugs and alcohol, etc.).

If Employees have any questions concerning these requirements including whether it is applicable to a particular website or social media platform, they should contact the Compliance

Officer and get an answer from the Compliance Officer prior to accessing or otherwise utilizing the website or service.

500 Global DocSend Policy

December 15, 2021

Policy Statement

As we move from a "control" to an "oversight" model with regard to Legal's involvement in distribution of fund marketing materials, the Firm is trusting its Employees to ensure compliance with all relevant fund marketing regulations. The key points to remember are:

- Fund marketing and diligence materials may only be distributed via a 500 Global Docsend account. Do not send such materials by email.
- Any in-person sharing of printed marketing materials would need to be logged in appropriate tracker sheets.
- Only fund marketing materials previously approved by Legal are permitted to be sent via Docsend.
- Existing US and international solicitation rules with regard to fund marketing materials will continue to apply (e.g. reverse solicitation evidence will still be required for certain jurisdictions).
- This Docsend Policy shall be a part and shall apply simultaneously with the Communication and Fund Marketing Policy.
- Legal will be actively auditing your usage of Docsend, failure to comply with this policy and the prescribed processes may lead to disciplinary action and termination of our Docsend license for all fund managers.

Workflow Overview

In the proposed new workflow, DocSend will allow fund managers and their teams to have more control over the distribution of fund materials subject to Legal's oversight. This new workflow will have two steps: 1) for distribution of one pagers / marketing decks; and 2) for distribution of substantive legal documents.

Stage 1: Marketing Decks and One Pagers

In line with market practice, fund marketing decks will now be shared via DocSend link so that potential investors may view the fund marketing decks without having to access a data room. Please note that this means that the fund marketing decks will be distributed **without potential investors first signing an NDA**. Previously investors went through our click-through NDA on Caplinked before being able to view the fund marketing deck. While, this new process is more in line with market practice, *this means that you should carefully consider whether there's any sensitive information that is included in your marketing deck (or any other materials such as a one page teaser) that should be reassessed, particularly surrounding portfolio company information*. In general, please be mindful of the information you include in your decks going forward.

Stage 2: Substantive Legal Documents (e.g. PPM, Summary of Terms, LPA etc.)

If a potential investor shows further interest in the fund, the investor can be added to the fund 'Space' (Docsend's version of a simplified VDR). Once added to the Space, the investor will be asked to verify their email address and sign our standard click-through NDA. The investor should then be able to access the Space without having to re-verify their email address so long as they do not clear their cookies.

Please see an overview of the workflows for Stage 1 and Stage 2 below.

Stage 1: Marketing Decks & One Pagers

1. Deck is uploaded as content on DocSend and a shareable link is created
2. Fund team shares this shareable link via email
    a. When sharing the link, please select "Require Email Verification"or specify the Domain for the recipient(s)
    b. The Account Name should be the full legal name of the fund (e.g. 500 Global __, L.P.) It is important that you use the correct Account Name so that all data is stored under one account. Accounts on DocSend cannot be combined or deleted.
    c. Consider using the DocSend Gmail integration so links can be added directly from Gmail
3. Whoever is sent the link is tracked in a Live Tracking Document that is checked by Legal periodically.

Stage 2:

Fund Space Creation

- Legal to create Template Fund Space and update as necessary;
- Legal will add fund team member who will create the Space as a collaborator to the template Space so that the fund team member can duplicate the template;
- Fund team member who wishes to receive an activity report should create the fund Space (and replicate Space settings). This is recommended as the creator of the Space appears on the Space's main page and also receives activity reports;
- Once the Space is created and ready to launch, the fund team member notifies Legal;
- Legal will upload the final versions of the fund documents to the Space.

Adding Potential Investors to the Fund Space

- Once the Space has been launched by Legal by uploading fund documents, each fund team member will be able to add potential investors to the Space via the "whitelist" function;
- After an investor is added to the whitelist, the fund team member will email the potential investor a link to the Space;
- Once a potential investor clicks on the link, they will be prompted to verify their email address and sign our click-through NDA; and

- If an investor has a due diligence request that requires sharing of more information with them, a new bespoke fund Space should be created for the investor.

Situations involving Reverse Solicitation

Reverse solicitation refers to a potential investor reaching out to 500 Global for more fund information on an unsolicited basis. Reverse solicitation is fact-based, meaning that either the investor truly requested fund information first or they did not. We rely on reverse solicitation in various jurisdictions because registering fund entities to market in those jurisdictions is costly and onerous, so fundraising teams should observe this while marketing in any jurisdiction which Legal identifies as requiring the use of a reverse solicitation exemption.

It is important to remember that while some jurisdictions have stricter reverse solicitation regimes than others, the cost of registering in these countries is often very high and involves robust annual reporting requirements. The costs associated with registration and any necessary reporting requirements will be charged back to the fund so fundraising teams should be cautious with fundraising from investors in any new jurisdiction. Please be aware that an investor is most likely to try and disprove reverse solicitation occurred when they are disgruntled or wish to divest from a fund. As such, it is in every fundraising team's best interest to ensure that a)the team checks with Legal on whether reverse solicitation requirements apply and b) the team maintains a clear record of an investor in a reverse solicitation jurisdiction having requested fund information from the team first.

Legal Oversight

While the legal team may have some limited supervisory rights with respect to Docsend access, the members of various fundraising teams have directly been provided Docsend authorizations with the expectation that in terms of the process of sharing materials via Docsend as well as the content of such materials, the members of fundraising teams will implement all the restrictions set forth in this Policy. . Please note, failure to comply with Legal's policies and procedures and the terms of this Policy may result in discipline or dismissal as well as the possible imposition of criminal, civil or administrative penalties.

Updates

This Policy and the Docsend Policy contained herein shall be updated from time to time as circumstances warrant.

Acknowledgement and Agreement

All Employees are required to sign the *Certificate of Acknowledgement and Agreement* attached in Exhibit A and return to the Compliance Officer.

EXHIBIT A
500 STARTUPS MANAGEMENT COMPANY, L.L.C.
Certificate of Acknowledgement and Agreement

Code of Conduct and Compliance Manual

I hereby acknowledge that I have read and understood the Code of Conduct & Compliance Manual adopted by 500 Startups Management Company, L.L.C and its affiliates and agree to fully comply with the policies and procedures set out therein including:

(i) Code of Conduct;
(ii) Policy Regarding Political Contributions dated December 15, 2021;
(iii) Insider Trading Policy dated December 15, 2021;
(iv) Information Security Policy dated December 15, 2021;
(v) Anti-corruption and Bribery Policy dated December 15, 2021;
(vi) Conflicts of Interest Policy dated December 15, 2021; and
(vii) Communications and Fund Marketing Policy dated December 15, 2021;

I hereby represent and warrant that I have truthfully and accurately disclosed any and all relevant disclosures required by the Code of Conduct & Compliance Manual and hereby agree to submit promptly and accurately any future disclosures required to the Compliance Officer.

I acknowledge that my failure to comply with such policies and procedures may result in my discipline or dismissal as well as the possible imposition of criminal, civil or administrative penalties.

_____ _____
Signature Date

_____
Name

_____
Title

EXHIBIT B
RELEVANT DISCLOSURES

In conjunction with the execution of the Certificate of Acknowledgement and Agreement set out in Exhibit A, upon joining the Firm, all Employees are also required to provide the following disclosures via Namely as part of their onboarding process:

(i) any political contributions to candidates for state or local government office in the United States in the past 24 months by you or a family member.
(NOTE: you do not need to disclose Federal or international political contributions).

(ii) any potential conflicts of interest including:

- any personal investments;
- any officer positions;
- any advisory engagements or other employment;
- any economic interests or personal relationships with limited partners / investors or Ecosystem clients;
- any economic interests or personal relationships with third party service providers;
- any economic interests or personal relationships with prospective or actual portfolio companies; or
- any other potential conflicts of interest that we should be aware of.

If you are unsure as to what you should disclose please discuss with the Compliance Officer prior to submitting the form.