AVEPOINT, INC.

POLICY ON INTERNAL INFORMATION BARRIERS

AND CONFIDENTIALITY

Last Reviewed and Approved: August 20, 2024

AvePoint, Inc., a Delaware corporation, (collectively with its subsidiaries, the "***Company***") is committed to administering a program of effective information barriers ("***Information Barriers***") to manage confidential information, and/or material non-public information ("***MNPI***") so as to provide a defense to what would otherwise be considered insider trading and to manage potential conflicts of interests in accordance with:

- applicable laws and regulations;
- the Company's obligations to its clients and counterparties; and
- measures for the protection of the Company's reputation.

Information Barriers are a crucial part of the regulatory system for public companies. They allow a diversified firm to conduct a variety of businesses which could not otherwise be conducted by the same firm. Information Barriers restrict the flow of information within a company to ensure that information which is potentially confidential or MNPI held in one division is not improperly communicated (including inadvertently) to any other division within the Company which is outside the relevant Information Barrier.

Accordingly, the Company's Board of Directors (the "***Board***") has established this Policy on Internal Information Barriers and Confidentiality (the "***Policy***"). While this Policy provides guidance as to how confidential information and MNPI should be managed and how Information Barriers should be built, maintained, administered, and overseen, each employee is personally responsible for determining whether they are in possession of confidential information or MNPI and ensuring that they act in accordance with this Policy. Remember: the end of a transaction does not always mean the end of confidentiality obligations.

Check with the Company's Office of the Chief Legal and Compliance Officer (the "***Office of the Chief Legal and Compliance Officer***") before assuming information obtained from a completed assignment may be MNPI, can be passed on internally or to a third party, or may be used for another purpose. This Policy is a supplement to the Code of Ethics and Business Conduct (the "***Code***") and should be read in conjunction with the Code**.**

A. APPLICATION OF POLICY.

While employees are encouraged to submit reports regarding any suspected violation of law or policy, this Policy details the minimum standards for the implementation and maintenance of Information Barriers within the Company. This Policy applies to all Company directors, officers, employees, contractors, secondees, and consultants wherever situated, and whether full-time, part-time or temporary (employees).

It is the responsibility of the relevant business units and internal teams to uphold and respect the

Information Barriers. The establishment or amendment of Information Barriers must only occur in compliance with this Policy and with consultation and approval from the Office of the Chief Legal and Compliance Officer and the Company's control room for policies and procedures generally (the "***Control Room***").

It is important that employees fully understand their personal obligations when in possession of confidential and/or inside information in order to maximize the effectiveness of this Policy.

B. INFORMATION SUBJECT TO THIS POLICY.

1. Confidential Information.

At any given time, the Company and its employees may hold information confidential to the Company or subject to confidentiality obligations (contractual or implied) to its clients, counterparties, or other parties. For legal and reputational reasons, it is essential that the Company maintains the confidentiality of such information entrusted to it by clients, counterparties, and other parties. Therefore, employees should treat all information at the Company as confidential information as it will almost always belong to the Company or a client.

Confidential information must not be communicated to anyone who does not have a legitimate "need to know" in connection with their work at the Company. Employees should therefore not make unauthorized disclosures unless:

a) disclosure complies with this Policy and any contractual obligations relating to the information;

b) the recipient has a legitimate need to know the information as part of their duties or to carry out a proposed transaction for a client;

c) the recipient understands the need to respect the confidentiality of the information and the limitations surrounding its use and disclosure;

d) the recipient does not have responsibilities that could give rise to a conflict of interest; and

e) disclosure will not breach relevant laws, regulations, and the Company's policies and procedures, including but not limited to the Code.

The need-to-know principle applies with equal force to those on the same side of the Information Barrier, and in cases when employees have been subject to a formal Crossing (as defined herein).

If confidential information is shared, the recipient of the information should be advised of its confidential nature and reminded that it should not be disclosed to anyone else in accordance with the need-to-know principle.

Certain clients, particularly governments and government agencies, have specific rules and detailed procedures with respect to the dissemination of confidential information. Employees who deal with such clients must be familiar with the relevant rules and procedures. Reference should also be made to the Company's "***Anti-Corruption Policy"***.

2. Material Non-Public Information.

From time to time, information received or acquired by the Company, or an employee may also constitute MNPI. MNPI can be generated within the Company while working with clients or counterparties or received inadvertently. Such MNPI is not always easy to recognize – indeed such information is often only recognized with hindsight and can be highly dependent on the individual facts and circumstances. The legal test as to what constitutes inside information may also vary between jurisdictions. Employees are encouraged to review the Company's "***Insider Trading Policy"*** and its "***Corporate Disclosure Policy"*** for more information on what may constitute MNPI.

When in doubt, employees should assume that the information is MNPI and contact the Office of the Chief Legal and Compliance Officer. As a guide only, and in conjunction with the Insider Trading Policy's and Corporate Disclosure Policy's further guidance on MNPI, employees can use the following questions to determine whether information may be MNPI:

a) Does the information relate directly or indirectly to:

   i. an issuer or issuers of financial products (i.e. a publicly traded company or a company that has currently traded or tradeable-in-future instruments like loans or derivatives?),

   ii. financial products, or

   iii. related products, whose price or value depends on a financial product(s)?

If 'yes':

b) Is the information non-public, that is, not generally available to users of the market for the relevant financial product? (*see* Insider Trading Policy for a discussion of what it means for information to be considered "Non-Public")

c) Is the information potentially price sensitive, that is, if it were made public:

   i. Would it have an effect on the price and/or value of the relevant financial product or related products?

   ii. Would a reasonable investor be likely to use this information as part of the basis for his or her investment decision to buy or sell the relevant financial product or related products?

   iii. Would a reasonable investor expect to receive the information in accordance with accepted market practice on the market in question?

A 'yes' response to any of these questions means information is likely to be MNPI.

The Office of the Chief Legal and Compliance Officer should be contacted for assistance in managing the possession of MNPI in accordance with the Insider Trading Policy and the Corporate Disclosure Policy.

3. If you have or are deemed to have MNPI. You are prohibited from:

a) trading;

b) providing advice; and

c) further disseminating the information (e.g.: tipping) or encouraging others to trade.

until such time as you no longer have or are deemed to have the relevant MNPI, or until you are advised by the Office of the Chief Legal and Compliance Officer that the information has been made public or become 'stale'.

Trading, disseminating, 'tipping', inducing, or encouraging others to trade while in possession of inside information in violation of applicable law may result in criminal liability, civil penalties or both.

C. INFORMATION BARRIERS.

1. What is an Information Barrier? A behavioral, contractual, legal, and sometimes physical wall (a "***Wall***") to prevent confidential information or MNPI held within one group or division of the Company from being communicated to another group or division outside the relevant group. Information Barriers allow the parts of the Company that do not possess confidential information or MNPI to continue to engage in their normal, day-to-day business activities. This is a key mechanism by which the Company ensures its clients' interests are protected and any conflicts managed. It is thus important that all employees follow the specific Information Barrier policies and procedures set forth below.

a) Information Barriers are essentially used to restrict the flow of inside information. In most jurisdictions, Information Barriers may provide a defense to activities which would otherwise be considered insider trading. They can also be used to manage potential or actual conflicts of interests that arise due to the diverse nature of The Company's business or to limit the flow of confidential information.

b) Some potential or actual conflicts of interest may not be managed by Information Barriers alone. As such, the use of Information Barriers in the management of potential or actual conflicts of interest should be carefully assessed by the business and in consultation with the Office of the Chief Legal and Compliance Officer.

2. Contractual Disclosures. In general, engagement agreements, terms of business, mandates and the like should include language that identifies the diversity of the Company's operations to the client and note that the Company, as a diversified publicly traded institution, may have a number of areas which may continue to trade securities issued by the client, including derivatives and related financial products. Agreements and mandates should note any specific activities where the Company's interests may conflict or potentially conflict with the interests of its clients. In some cases, explicit consent may be required from a client with respect to a transaction that may give rise to an actual or potential conflict of interest as part of the measures to manage an actual or potential conflict of interest.

3. Physical and Behavioral Measures. The Company is required to have appropriate systems, controls and procedures in place to ensure that it handles confidential information properly and safeguards it to prevent misuse. Accordingly, The Company's Information Barriers are supported and reinforced

through physical and behavioral measures.

a) Examples of physical measures include:

i. the separation of business groups or divisions with Information Barriers;

ii. restricted swipe card access to buildings and floors; and

iii. restricted computer system and file access.

b) Examples of behavioral measures include:

i. clear desk requirements, such as the secure storage of documents and other material containing confidential and/or MNPI;

ii. not discussing confidential and/or inside information outside of the relevant Information Barrier area, or in public places such as elevators and shared kitchens; and

iii. being mindful of additional procedures concerning disclosure of MNPI due to industry risk, high profile transactions, publicly traded third parties, or government body involvement, or contractual restrictions in relation to particular information.

It is the direct responsibility of each employee to observe both the physical and behavioral elements of the Company's Information Barriers.

4. Public Side vs. Private Side Groups. Certain Company businesses routinely receive or acquire, or distribute or create, information in relation to their activities and the activities of clients or counterparties which is not generally available and is potentially price-sensitive to the value of relevant financial products, including securities, their derivatives and other related financial products.

a) *Private Side*. The business areas that routinely receive or acquire, or are integral to the distribution of, confidential information and/or MNPI from the Company or its customers or clients are on the "***Private Side***" of the Information Barrier.

b) *Public Side*. Those business areas that deal with third parties and internal groups on the basis of publicly available information (i.e. no MNPI) are on the "***Public Side***" of the Wall. Be aware that despite this nomenclature, employees of AvePoint Public Sector, Inc. (a subsidiary of the Company) may come into possession of MNPI and, depending on their business area within that entity, maybe Private Side or Public Side, as applicable.

5. Special Purpose Information Barriers.

"***Special Purpose Information Barriers***" are temporary arrangements that may be used to address a specific business objective for a finite time. However, there are strict requirements that must be met in order to establish an effective Information Barrier and as such, the Office of the Chief Legal and Compliance Officer and the Control Room should be consulted in their establishment. Examples of special purpose Information Barriers include but are not limited to:

a) when a business acquisition of a listed entity is being contemplated by a public side part of the Company;

b) when a private side business is setting up separate deal teams with respect to a potential sale of Company assets, business lines, or equity; or

c) transactions that are potentially price-sensitive to the Company, such as significant business or asset acquisitions.

6. General. In the absence of an effective Information Barrier, if one part of the Company received confidential information or MNPI, **that information may be attributed or attributable to every other part of the Company**, even when other areas do not actually possess the information. The Company and each employee could therefore be unable to trade in that information or provide advice on the relevant securities, even where such information is directly related to the Company itself.

D. WALL CROSSING.

1. General. In certain circumstances, Private Side employees may need to obtain the advice or assistance of a Public Side employee. Contacts of this type are permitted so long as MNPI is not disclosed to the Public Side employee. If it becomes necessary or advisable for a Private Side employee to disclose MNPI to a Public Side employee ("***Wall-Crossing***"), the Private Side employee must follow the Wall-Crossing procedures prior to disclosing information that is or may be MNPI. Note: In some cases, the very fact that the Company is working on an engagement for a particular client may constitute MNPI. Wall-Crossing procedures allow for limited and controlled disclosure of MNPI to Public Side employees for specific purposes, while continuing to preserve the confidentiality of MNPI.

2. Procedures. The Chief Legal and Compliance Officer will consider the following factors in evaluating a proposed Wall-Crossing:

a) The importance of the proposed Wall-Crossing's objective;

b) The need to know of the proposed person to be Wall-Crossed;

c) The availability of other means to accomplish the objective;

d) The timing and duration of any proposed transaction;

e) Potential adverse impact on Public Side activities, e.g., restrictions on trading, supervisory responsibilities; and

f) Any threats the proposed Wall-Crossing may pose to the integrity of the Information Barrier.

If approval is granted by the Chief Legal and Compliance Officer, the information disclosed to a Wall-Crosser (defined below) should be limited to need-to-know information that is required in order for the Wall-Crosser to carry out their work for the Private Side project. Any other limitations imposed by the Chief Legal and Compliance Officer must also be observed.

The Chief Legal and Compliance Officer is responsible for overseeing the Wall-Crossing process and will maintain a record of all Wall-Crossings and coordinate with the Control Room to do so. The record will include the name of the Wall-Crosser, the name of the counterparty issuers involved, the name of the person requesting the Wall-Crossing, and relevant dates.

3. Wall-Crossers.

a) A Public Side employee who has crossed the Wall (a "***Wall-Crosser***") is treated as a Private Side employee for purposes of this Policy for the particular purpose of the Wall-Cross, so long as they possess MNPI that has not been made public, become stale or otherwise immaterial. The Public Side employee properly authorized to cross the Information Barrier will receive a Policy reminder regarding handling of MNPI and the manner in which his or her activities may be limited.

b) A Wall-Crosser's Public Side activities will be restricted with respect to any security or other financial instrument to which any MNPI they receive relates or is affected, unless advised otherwise by the Chief Legal and Compliance Officer.

c) The Wall-Crosser may not be able to participate in day-to-day investment or trading decisions regarding any security or other financial instrument relating to the Wall-Crossing, if advised by Chief Legal and Compliance Officer. These activities, however, may continue on the Public Side of the Information Barrier without the participation of the Wall-Crossed individual.

d) A Wall-Crosser may return to their Public Side duties with respect to the relevant customer, counterparty, issuer, security, or offering when the MNPI they received has been made public or as otherwise advised by the Chief Legal and Compliance Officer. No further disclosure of MNPI may be made to the Public Side employee following return to the Public Side of the Information Barrier unless a new request is submitted and approved for the proposed Wall-Crossing.

4. Restrictions on Communications. Where an Information Barrier exists, an employee on one side of the barrier may not communicate (or otherwise give access to) information acquired or created in that business area to an employee on the other side of the Information Barrier except in accordance with specific Wall-Crossing procedures and with the prior authorization of the Office of the Chief Legal and Compliance Officer or the Control Room. Physical access restrictions reinforce the information barriers.

The Office of the Chief Legal and Compliance Officer or the Control Room may approve communications otherwise prohibited hereunder subject to such conditions as they may deem appropriate to ensure that Private Side employees will not communicate to employees of another Public Side sector any MNPI with respect to the Company or identified issuers of publicly traded securities. Examples of conditions that may be deemed appropriate on a case-by-case basis include monitoring of oral communications by the Office of the Chief Legal and Compliance Officer, limiting the subjects to be addressed in oral communications, pre-clearing written communications and requiring use of code names in oral and written communications. The Office of the Chief Legal and Compliance Officer or the Control Room shall maintain a log of such approved cross-wall communication.

The Information Barrier does not prevent communications regarding information that is not

confidential or is already public.

5. Inadvertent Wall-Crossing. A Public Side employee who obtains information they believe may be MNPI without an appropriate Wall-Crossing approval should immediately notify the Chief Legal and Compliance Officer or his designee. Unless advised to the contrary by the Chief Legal and Compliance Officer, the employee should refrain from engaging in, soliciting or recommending transactions in the related securities or other financial instruments for any account (whether for the Company, a client, a personal account or any other account) and avoid further disclosure of the information.

6. Above-The-Wall Employees.

a) Employees who because of their senior management positions or because they serve a risk function across businesses (e.g. legal, compliance, data privacy, etc.) may be designated as "above-the-wall" ("***ATW***").

b) ATW employees will potentially have information across all Information Barriers. These employees or divisions will often have employees and/or businesses on both the public and private side of the Information Barrier reporting to them and therefore may obtain inside information without the use of Information Barrier crossing procedures. Since these special Information Barrier privileges, therefore only the ATW employees have Office of the Chief Legal and Compliance Officer (or their delegate), may approve an employee's or a division's ATW status.

c) *ATW Responsibilities*.

i. Employees with ATW status must not communicate confidential information or MNPI obtained from one Information Barrier area to employees outside that Information Barrier area. They must also not participate in activities that involve trading or the provision of financial product advice and may need to disqualify themselves from participation in such decisions more generally.

ii. Although there is a presumption that ATW employees have information that rests across Information Barriers, the "Need to Know" principle must be strictly observed when communicating with ATW functions. This is because being in an area that is designated ATW does not necessarily entitle those employees to receive all confidential information or MNPI, such as file or floor access to all business groups.

iii. Employees who are considered ATW, for example the Company's Senior Leadership Committee members, may speak to other employees who are also ATW without a Wall-Crossing.

E. OTHER INFORMATION CONTROLS.

1. "Need to Know" Policy.

a) The Company has a "need to know" policy with respect to the disclosure of confidential information and inside information. Employees are expected to limit the access to and

disclosure of such information to those persons who:

i. must have the information to serve the proper business purposes of the Company, or

ii. must have the information to serve the proper business purposes of clients, and

iii. can be expected to maintain the information in confidence.

b) The people that may "need to know" should be those that are:

i. personnel and external advisers directly involved in the transaction with the client,

ii. managers of people that are involved in the transaction, and

iii. fulfilling corporate control functions

c) Employees must not disclose:

i. Confidential information to any person under any circumstances in which it appears likely that such person will misuse the information, and

ii. MNPI, except as permitted herein.

2. Protecting Confidential Information and MNPI.

a) Access and Communication.

i. To the extent possible, access to office areas where confidential and/or inside information may be observed or discussed should be limited to persons with a business reason or purpose for being in the area. It is Company policy that areas where confidential information and MNPI is accessible or stored shall be appropriately segregated and secure.

ii. Mobile phones, e-mails, and other means of electronic communications may not be secure. Employees should use them with care. Employees may only use Company-authorized e-mail and instant messaging systems when discussing confidential information or information that may be MNPI.

iii. Employees should not discuss confidential information and/or MNPI in public places such as hallways, elevators, taxis, airplanes, airports, subways, trains, and restaurants. Speaker phones should not be used in circumstances where confidential information may be overheard.

b) Visitors. Visitors should not be allowed to frequent private areas of the Company unescorted; rather, visitors should be escorted to their destination. Visitors attending meetings at the Company should not be permitted access to areas not related to the purpose of their meeting. As a general rule, visitors should not be allowed unattended in the offices

of professional employees or other areas where they may be exposed to confidential and/or non-public information.

c) Documents and Materials.

i. Employees must safeguard documents and other materials that contain confidential information or MNPI. These should not be left exposed to public access. Whenever possible, such materials should be stored in desks or file drawers, cabinets, or otherwise secured from public access when not in use. When in use, employees should be careful not to leave such documents unattended unless precautions are taken to secure them from public access.

ii. Whenever possible, materials containing confidential information and/or MNPI sent to the duplicating or telecommunications staff should be transmitted in interoffice envelopes. When such materials are delivered throughout the office, for example to an employee's desk or in-box, they should be placed face down.

iii. Other documents that disclose client identities, such as client lists, working group lists, code name lists, and number lists should be maintained and destroyed with similar care.

d) Materials Outside the Office. When materials containing confidential information and/or MNPI are taken from the office, employees should be careful to ensure that such materials are secure from public view. Materials containing confidential information and/or MNPI should be removed from the Company's offices only for bona fide business reasons. Whenever it is possible to avoid doing so, such materials should not be discarded outside of the Company's offices.

F. OFFICE OF THE CHIEF LEGAL AND COMPLIANCE OFFICER.

The Company's Chief Legal and Compliance Officer may be reached at 1-804-314-5903 or brian.brown@avepoint.com. The Chief Legal and Compliance Officer is responsible for administering this Policy in conjunction with the Control Room. The Chief Legal and Compliance Officer may also designate additional individuals to assist them in carrying out all duties of the Chief Legal and Compliance Officer required by this Policy. The Chief Legal and Compliance Officer is responsible for monitoring, overseeing, and investigating breaches of this Policy.

G. REVIEW OF POLICY.

Each new executive officer and director of the Board (each, a "***Responsible Person***") shall be required to review a copy of this Policy and to acknowledge in writing that he or she has done so. Any amendments to this Policy, from time to time, shall be communicated immediately to all Responsible Persons.