AVEPOINT, INC.

EXPORT CONTROL AND TRADE SANCTIONS COMPLIANCE POLICY

LAST REVISED AND APPROVED: DECEMBER 11, 2024

I. PURPOSE AND POLICY STATEMENT

AvePoint, Inc., a Delaware corporation, (collectively with its subsidiaries, the "***Company***") is committed to complying fully with all applicable laws and regulations related to export controls and trade sanctions. The purpose of this Export Control and Trade Sanctions Policy (the "***Policy***") is to facilitate compliance by the Company with all applicable trade laws, including, but not limited to, the U.S. Export Administration Regulations, the U.S. International Traffic in Arms Regulations, U.S. sanctions regulations administered by the U.S. Treasury Department's Office of Foreign Assets Control, Council Regulation (EC) No 428/2009 (as amended) (the "***E.U. Dual-Use Regulation***"), E.U. sanctions regulations, the U.K. Export Control Order 2008, the U.K. Sanctions and Anti-Money Laundering Act 2018, U.K. sanctions regulations and similar applicable laws in any other jurisdictions where the Company conducts business (collectively, "***Export and Sanctions Laws***").

This Policy applies to all directors, officers, employees, and agents of the Company (collectively "***Representatives***"). All Representatives must comply with all applicable Export and Sanctions Laws and are prohibited from (1) manipulating any transaction, service arrangement, relationship, or document to circumvent this Policy; or (2) facilitating or advising anyone regarding the circumvention of Export and Sanctions Laws or this Policy.

Failure to comply with this Policy and any applicable Export and Sanctions Laws could lead to business disruption, harm to the Company's reputation, loss of export privileges, and/or significant civil and criminal penalties for the Company and Representatives, including individuals. Representatives who violate this Policy are subject to appropriate disciplinary action, including demotion, reassignment, additional training, probation, suspension, or even termination (and may themselves face criminal prosecution from the relevant authorities, which may lead to fines and/or imprisonment).

II. COMPLIANCE OFFICER

The Company has appointed a Compliance Officer ("***Compliance Officer***") who is responsible for ensuring the Company's compliance with this Policy and applicable Export and Sanctions Laws. The Compliance Officer reports to the Company's Board of Directors. In addition to the specific duties set forth herein, the Compliance Officer has full authority to implement and enforce this Policy, which will be updated on a regular basis with associated training.

III. EXPORT CONTROL LAWS

A. Export Controls

Controls apply to the 'export' of certain products, software and technology (including their transfer cross-border).

These items are deemed to be strategically sensitive and accordingly listed under the exporting country's export control laws/regulations, examples of which include the U.S. Export Administration Regulations ("***EAR***"), the E.U. Dual-Use Regulation and U.K. export control laws (together, "***Export Control Laws***").

It is also important to be aware that software and technology in this context can have a broad meaning:

- "Software" means a collection of one or more "programs" or "microprograms" fixed in any tangible medium of expression.
- "Technology" means specific information necessary for the "development", "production" or "use" of goods. This information takes the form of "technical data" or "technical assistance". Common examples include diagrams, blueprints, technical specifications, knowhow, manuals, instructions, etc.

Transfers covered include both:

- the physical transfer of goods, software of technology, where items are sent or carried across borders; and
- the intangible transfer of software or technology, for example, transfer by email, fax, electronic download, internal network, phone/video conferencing or transfer via cloud storage and software repositories.

Export Control Laws apply not only to transfers made to third parties in a commercial context, but also to those made internally within a company or within a group of companies (e.g. for R&D purposes).

Some of the Company's products, software, and technology are controlled under Export Control Laws. The Compliance Officer will work with relevant Company personnel and/or outside counsel to determine the export classification of the Company's products, including the applicable classification number under the Export Control Laws (for example, their Export Control Classification Number or ECCN for the purposes of the EAR), destination controls, and any associated licensing, classification or reporting requirements.

1. Encryption

Certain of the Company's products and technology incorporate encryption functionality, exports of which are restricted under many export control regimes.

The EAR prohibit the export of certain encryption items without obtaining a commodity classification (also known as a CCATS) and/or license from the U.S. Commerce Department. Most encryption items are eligible for export without obtaining a specific license under License Exception ENC or because the item's limited use of encryption falls within an exemption to the EAR's encryption controls. Exports under License Exception ENC may be subject to classification and/or reporting requirements.

Similar restrictions are also in place in respect of E.U., U.K. and other global Export Control Laws: if these controls apply and there is no relevant exemption, a license to export will be required.

As discussed above, the Compliance Officer will determine the export classification of the Company's products, including whether they are subject to encryption controls.

2. Deemed Exports to Foreign Nationals in the United States

Disclosure of technology, including software source code, to foreign persons in the United States, including foreign national employees of U.S. companies, is considered a "deemed export" under the EAR. It is important to note that export transactions are not limited to the physical export of products outside of the United States. For these purposes, a foreign national is any person who is not a U.S. citizen or permanent resident alien (i.e., green card holder), or a "protected individual" under 8 U.S.C. § 1324b(a)(3).

Before the Company engages in an activity that could result in a deemed export, such as the employment of a foreign national or receipt of foreign national visitors, the Compliance Officer must be consulted to ensure that any required export license is obtained prior to the disclosure of export controlled technology to a foreign person.

3. Exports of Software and Technology Including Offshore Development

Exports of certain Company software and technology, such as source code in connection with offshore software development activities, may require a license or other governmental authorization prior to export (which can include intangible exports such as transfers to persons in other countries or uploading software and technology to servers accessible to persons in other countries). You must consult with the Compliance Officer prior to verbally communicating or electronically transferring any Company software and technology, including source code or technical information necessary for the development or production of the Company's products, to another country. This applies whether the transfer is being made internally within the Company or to a third party.

B. End-Use Prohibitions and Red Flags

Products or technology destined for certain end uses or end users may be subject to restrictions and/or licensing requirements under Export Control Laws, even if the product or technology would not otherwise be subject to licensing requirements. Restricted end-uses include uses directly or indirectly in connection with (i) activities involving chemical, biological or nuclear weapons, missiles or other nuclear explosive devices; (ii) military activities, such as when the destination is subject to an arms embargo or the transaction involves items which have been illegally exported; (iii) terrorist activities; or (iv) cyber surveillance activities, particularly concerning regimes involved in internal repression or human rights abuses.

Company personnel must be alert to any circumstances or "red flags" indicating that an export may be destined for a prohibited end use, end user, or destination (including where a proposed customer may be involved in such activities). The U.S. Commerce Department publishes a list of such "red flags" at https://www.bis.doc.gov/index.php/enforcement/oee/compliance/23-compliance-a-training/51-red-flag-indicators; the U.K. Export Control Joint Unit publishes a similar list in Annex 5 to its Compliance Code of Practice, see https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/341998/10-668-codepractice-compliance.pdf.

If you have reason to know or suspect, or any grounds for suspecting, that a transaction may involve a prohibited end use, you must stop all activity and consult with the Compliance Officer. No Company personnel is permitted to complete any transaction, shipment, or release of technology that has been identified as a suspect transaction or that involves a "red flag," until after it is reviewed and approved by the Compliance Officer. Immediately stop all activity and seek assistance of the Compliance Officer when a potential compliance issue is spotted.

C. Military and Defense Items and the International Traffic in Arms Regulations

Exports and reexports of defense articles, services, and technical data are regulated under relevant controls on military items in a number of countries the Company operates in, including the U.S. State Department's Directorate of Defense Trade Controls under the International Traffic in Arms Regulations ("***ITAR***"). Products, software and associated technical data that is specially designed, modified, configured, adapted, or prepared for use in certain military, intelligence, or satellite applications, or for a customer engaged in these activities, may be controlled under the ITAR or other military export control laws and require a license before export to any destination.

The Company generally does not produce, receive, or export defense items. If you believe that a particular transaction or dealing may involve ITAR or other military-controlled products or technical data, please consult with the Compliance Officer before proceeding.

IV. TRADE SANCTIONS

Many of the countries in which the Company is active administer trade sanctions prohibiting certain economic activities in relation to various countries, individuals and/or entities. These sanctions are enforced at country level by government authorities, including the U.S. Treasury Department's Office of Foreign Assets Control ("***OFAC***") in the U.S. and the Office for Financial Sanctions Implementation in the U.K. E.U. sanctions are enforced by authorities at Member State level. Different types of trade sanctions include the following:

- **Country-specific sanctions and embargoes** can include broad prohibitions against direct or indirect (through third parties) transactions and business activities involving certain countries and, in some cases, all government and non-government entities and individuals located or resident therein. For example, comprehensive country-specific sanctions maintained by the United States restrict a broad range of economic activities in the specified countries and these countries are therefore typically very high risk from a compliance perspective. The E.U. and U.K. also maintain extensive sanctions against certain countries. Countries targeted by comprehensive or extensive country-specific sanctions currently include Cuba, Iran, North Korea, Syria, and the Crimea region of Ukraine (collectively, the "***High Risk Sanctioned Countries***", the list of which is maintained and updated by the Compliance Officer). Dealings with these countries can also give rise to risks under broader compliance laws as well as practical or commercial difficulties.

  No transactions or dealings may proceed with High Risk Sanctioned Countries or government and non-government entities and individuals located or resident therein, unless authorized in advance in writing by the Compliance Officer. If you believe that a transaction or dealing may directly or indirectly involve a High Risk Sanctioned Country, please contact the Compliance Officer immediately before taking any further steps.

- **List-based sanctions** prohibit or restrict direct or indirect (through third parties) transactions with certain entities and individuals that appear on certain relevant restricted party lists. These include the Specially Designated Nationals and Blocked Persons List, the Foreign Sanctions Evaders List, and the Sectoral Sanctions Identifications List in the U.S.; the European External Action Service ("EEAS") Consolidated List of Sanctions in the E.U.; and the U.K. Consolidated List Of Financial Sanctions Targets and the U.K. Sanctions List in the U.K. (collectively, the "***Sanctions Lists***").

No transactions or dealings may proceed in any country with persons on relevant Sanctions Lists (or with non-listed persons which are owned or controlled by persons on relevant Sanctions Lists), unless authorized in advance in writing by the Compliance Officer. If you believe that a transaction or dealing will directly or indirectly involve a person on a Sanctions List, please contact the Compliance Officer immediately before taking any further steps.

- **Sectoral or other country-based sanctions** prohibit certain types of direct or indirect (through third parties) transactions impacting certain listed parties or sectors of a country's economy. The most relevant types of these sanctions include the U.S. Sectoral Sanctions Identification List and the E.U. and U.K. sanctions against Russia, both of which target certain sectors of the Russian economy, including the financial services, energy, defense and related material sectors. In most cases, only certain types of transactions involving a designated entity, e.g., the purchase of new debt or equity, are prohibited. In addition, OFAC administers limited sanctions against the Government of Venezuela and Petroleos de Venezuela, S.A., the Venezuelan state-owned oil and natural gas company. Certain other countries and territories are targeted by material sanctions, including those relating to Belarus and Myanmar. A list of such "***Medium Risk Sanctioned Countries***" is maintained and updated by the Compliance Officer).

You must consult the Compliance Officer before engaging in any transaction potentially involving, directly or indirectly, (i) a High Risk Sanctioned Country, or their nationals (wherever located), (ii) a Medium Risk Sanctioned Country, or (iii) any entity or individual on a Sanctions List (or owned or controlled by a person on a Sanctioned List).

To comply with this Policy, the Company has implemented procedures for screening its customers, vendors, and partners against the Sanctions Lists, as described in Section V. below.

V. RESTRICTED PARTY SCREENING

The Company will screen customers, resellers, and distributors against relevant Sanctions Lists and other applicable restricted party lists, including the Denied Persons List, the Unverified List, and the Entity List, maintained by the U.S. Commerce Department's Bureau of Industry and Security, the EEAS Consolidated List of Sanctions, the U.K. Consolidated List Of Financial Sanctions Targets and the U.K. Sanctions List (collectively, the "***Restricted Party Lists***"). The Company will screen parties before on-boarding or entering into a relationship, and thereafter on a periodic basis.

The Compliance Officer will be responsible for managing the Restricted Party Screening process and delegating persons, as appropriate, to conduct the screening and to review screening results.

VI. U.S. ANTI-BOYCOTT RULES

The U.S. Commerce Department and the Internal Revenue Service ("***IRS***") administer rules governing compliance with non-approved international boycotts, particularly the Arab League boycott of Israel. U.S. companies and their controlled foreign subsidiaries or branches are not permitted to comply with requests for information that support unauthorized boycotts. Other prohibited boycotts may involve boycotts on India or Pakistan. A boycott request may take the form of a questionnaire, an informal written request for information, or a certification requirement. The mere receipt of boycott requests often must be reported.

Under these laws, the following actions are prohibited:

- refusing to do business with a boycotted country, nationals or companies of a boycotted country, or

"blacklisted" companies;

- furnishing boycott-related information, including information about business relationships with a boycotted country, nationals or companies of a boycotted country, or "blacklisted" companies;
- discriminating against any U.S. person on the basis of race, religion, sex, or national origin;
- agreements to refuse to do business directly or indirectly within a country or with a country's government, companies or nationals;
- agreements to refuse to do business with U.S. persons who do business in a country or with its government, companies, or nationals;
- agreements to refuse to do business with companies owned or managed by individuals of a particular race, religion, or nationality;
- agreements to refrain from employing persons of a particular race, religion, or nationality; and
- agreements to refuse to ship or insure products on carriers owned or operated by persons who do not participate in or cooperate with the boycott.

You must not respond to questionnaires or other requests for information regarding the Company's business activities with or concerning Israel (or any similar request regarding India, Pakistan, or other countries subject to unapproved boycotts). If you receive such a request, you must not respond or take any further action until you have consulted with the Compliance Officer. The Compliance Officer will prepare and submit any required reports to the U.S. government, and contact the Company's tax preparer to ensure compliance with IRS regulations.

VII. CONFLICTS BETWEEN LAWS

It is important to be aware that, due to the global nature of the Company's business, there will be some instances where the sanctions policies of two or more countries in which the Company operates may conflict. Those transactions will need to be carefully assessed to ensure the Company is compliant.

For example, E.U. Council Regulation (EC) No 2271/96 (the "***E.U. Blocking Regulation***") prohibits E.U. operators (as defined in the Regulation) from directly or indirectly complying with extra-territorial U.S. sanctions against certain countries, including Iran and Cuba. The U.K., Canada and Mexico maintain similar laws.

Any transactions involving a conflict between laws, or with a nexus to Iran or Cuba, must be immediately referred to the Compliance Officer before any further steps are taken.

VIII. RECORDKEEPING

Recordkeeping is an essential part of the Company's compliance with applicable Export and Sanctions Laws.

U.S. export control laws require that records of covered transactions be maintained for a period of five years from the latter of the date of export, the exhaustion of the export license authorizing the transaction, or the

expiration of the export license or authorization. The Export and Sanctions Laws of other jurisdictions (including the E.U. and the U.K.) also set out strict record keeping requirements which must be complied with.

To comply with the above requirements, the Company shall keep and maintain internal records pertaining to its export transactions and compliance efforts regarding Export and Sanctions Laws for at least five years or such other period as may be required by applicable law. Records must be retained in accordance with applicable local legal requirements. These will generally include, but are not limited to, books of account, contracts, standing instruction records, letters, email, memoranda or other papers connected with a transaction. In the case of transactions subject to export controls, these will typically need to clearly record the nature of the export (including how the item was exported, description of the items that were exported, the dates of export and quantity of the items) and any persons involved in the export (person making the export, consignee, recipient, end-user and any supplier that is involved).

You should consult with the Compliance Officer if you have any questions regarding whether particular documents are required to be maintained, or whether the retention period for a transaction has expired.

IX. UPDATES AND TRAINING

The laws and regulations governing the Company's compliance obligations are subject to frequent change with little or no notice. The Compliance Officer and/or outside counsel will review this Policy on a periodic basis and update it, as appropriate, to reflect any changes.

Periodic compliance training will be provided to relevant Representatives to ensure that they are familiar with applicable Export and Sanctions Laws and the Company's internal procedures.

X. REPORTING AND QUESTIONS

Representatives have an affirmative obligation to report any apparent or suspected violations or circumventions of this Policy, including by a third party, to the Compliance Officer as follows:

Brian Michael Brown

Phone: (804) 314-5903

Email: brian.brown@avepoint.com

The Company will ensure that appropriate confidentiality measures are taken and will not retaliate against any individual for reporting violations in good faith.

We welcome any comments or questions that you may have regarding the substance and implementation of this Policy. Please direct such communications to the Compliance Officer.