FIVE BIOENERGY
BALANCED WITH THE PLANET

SANCTIONS AND EXPORT CONTROLS COMPLIANCE POLICY

FIVEBIOENERGY, S.L.

3 December 2025

Fivebioenergy, S.L., and its subsidiaries, (collectively, the "**Company**" or "**Fivebioenergy**") is committed to doing business consistent with the highest ethical standards and legal requirements everywhere the Company operates, and expects all Company management, employees, and other persons acting on the Company's behalf to uphold this commitment. Consistent with this commitment, the Company has adopted this Sanctions and Export Controls Compliance Policy (the "**Policy**"), which outlines the Company's responsibilities to comply with the economic sanctions laws and regulations. It is the Company's policy to comply fully with these legal requirements. Therefore, all directors, officers, employees, and other agents are responsible for understanding and complying with the terms of this Policy in the performance of their duties.

Compliance with the Company's highest ethical standards and legal requirements is a shared responsibility and key to who we are. The Policy provides a general guide to Sanctions and Export Controls but does not address every potential scenario that we may face. Anyone with questions concerning Sanctions or Export Controls (as these terms are defined below) or the requirements of this Policy should consult with the Compliance Risk Committee.

The Company requires all directors, officers, employees, and other agents to report any conduct that may violate Sanctions, Export Controls or this Policy, in accordance with the procedures identified below.

I. STATEMENT OF POLICY

Fivebioenergy is committed to compliance with all applicable laws and regulations, including those related to sanctions ("**Sanctions**") and export controls ("**Export Controls**"), as described below. This Policy is focused on Sanctions and Export Controls compliance and requires that the Company, including its management, employees, and third-party partners acting on its behalf (collectively "**Covered Persons**"), do not:

- engage in any business with, sell any products or provide any services to persons or entities that are designated on any sanctioned party lists maintained by the United Nations, the European Union, the United Kingdom, the United States or other applicable jurisdictions, unless authorized by the Company's Chief Executive Officer ("**CEO**") and the Compliance Risk Committee (as this term is defined below) or relevant governmental authorities;

- sell any products or provide any services to, or otherwise do business involving any jurisdiction that would violate the Sanctions restrictions of the United Nations, the European Union, the United Kingdom or the United States, alongside any other national Sanctions regime relevant to the transaction in question, unless authorized by

the Company's CEO and ESG Responsible or relevant governmental authorities; or

- export or reexport any items (good, technology, or software) or transfer items to third party nationals in violation of any Export Controls administered by the European Union, the United Kingdom, the United States or any other applicable jurisdiction.

Any exceptions to this Policy must be consistent with applicable laws and will be made only with the explicit written approval of CEO.

Violations of this Policy by any director, officer, employee or third-party agent or partner of the Company will result, among other measures or remedies, in appropriate disciplinary actions up to and including termination of the corresponding employment, agency or commercial agreement. Failure to comply with applicable Sanctions or Export Controls may result in significant criminal, civil, and administrative penalties, including imprisonment and fines. Any suspected violations of this Policy should be reported to the Compliance Risk Committee of Fivebioenergy (the "**Compliance Risk Committee**").

If you have any questions about your obligations to comply with Sanctions, Export Controls and this Policy, or if you suspect that any violation has occurred, you should contact the Compliance Risk Committee.

II. OVERVIEW OF SANCTIONS

As discussed above, it is the Company's policy to comply with all Sanctions administered by the United Nations, the European Union, the United Kingdom, the United States and any other jurisdictions, as applicable. In the event of any conflict of laws, the Compliance Risk Committee should be consulted.

Under certain circumstances, the Company also has an obligation to ensure that its third-party partners are conducting business on its behalf in compliance with all applicable Sanctions.

With respect to the restrictive measures of the European Union's common foreign and security policy ("**EU Sanctions**"), the European Union adopts over forty separate sanctions regimes. EU Sanctions are legislated at an EU-wide level by the Council of the European Union, but are primarily enforced by national states. EU Sanctions encompass a range of restrictive measures, including asset freezes, travel bans, export restrictions and sectoral embargoes.[1]

[1] A map illustrating current EU Sanctions can be found here https://www.sanctionsmap.eu/#/main, and a consolidated list of persons, groups and entities subject to EU Sanctions can be found here https://data.europa.eu/data/datasets/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions?locale=en.

Since 31 December 2020, the United Kingdom has operated a number of autonomous sanctions regimes outside the European Union. Whilst the United Kingdom continues to adopt many EU Sanctions in full, the UK sanctions list diverges from the list of persons and entities subject to EU Sanctions, and must be complied with separately.[2] UK sanctions are now primarily administered by HM Treasury, and enforced by the Office of Financial Sanctions Implementation.

Although the Company is not a U.S. company, it may engage in transactions with a U.S. nexus (including transactions involving U.S. citizens, U.S. lawful permanent residents, persons located in the United States, and U.S.-incorporated entities and their non-U.S. branches, U.S.-origin goods or services, or the U.S. financial system (*i.e.*, transactions conducted in U.S. dollars)). Therefore, as a matter of policy and to mitigate risk, the Company will abide by U.S. sanctions requirements across all of its business operations, even with respect to transactions that do not involve U.S. dollars or another U.S. nexus, alongside its other legal obligations to the sanctions requirements of the United Nations, the European Union and the United Kingdom.

With respect to applicable U.S. Sanctions, the U.S. Department of the Treasury, Office of Foreign Assets Control ("**OFAC**") is the primary U.S. government agency responsible for administering Sanctions.

OFAC maintains three types of sanctions programs, as follows:

A. **Comprehensive Sanctions**. OFAC currently administers comprehensive economic sanctions against **the Crimea, Donetsk and Luhansk regions of Ukraine, Cuba, Iran, Syria, North Korea and Venezuela**.[3]

B. **List-Based Sanctions**. OFAC sanctions entities and individuals designated on OFAC's sanctions lists, including the Specially Designated Nationals and Blocked Persons List (the "**SDN List**").[4] Entities and individuals are placed on the SDN for a variety of reasons, including having been determined to be connected or associated with or participating in certain illicit activities, such as international terrorism, proliferation of weapons of mass destruction, sanctions evasion, international drug trafficking and other transnational crime, human rights abuses, corruption, and malicious cyber

[2] The UK sanctions list of financial sanctions targets can be found here https://www.gov.uk/government/publications/the-uk-sanctions-list.

[3] In the case of Venezuela, OFAC has sanctioned the Venezuelan government (including government officials and government-owned entities) rather than the entire country. However, given the pervasive role the Venezuelan government plays in the Venezuelan economy, you must consult the Company's legal department in advance to determine whether any transaction involving Venezuela is permissible.

[4] The SDN List is available here https://sanctionslist.ofac.treas.gov/Home/SdnList. Other OFAC sanctions lists also are available here https://ofac.treasury.gov/other-ofac-sanctions-lists.

activities. **Importantly, OFAC considers any entity 50% or more owned in the aggregate by individuals or entities identified on the SDN List to be "blocked" and subject to the same restrictions as SDNs, even if the entity is not itself designated on the SDN List.**

Furthermore, as of the date of this Policy, OFAC has placed individuals and entities on the SDN List for engaging in conduct relating to the following countries and regions: **Afghanistan**, **Balkans, Belarus, Central African Republic, China, Darfur, Democratic Republic of the Congo, Ethiopia, Hong Kong, Iraq, Lebanon, Libya, Mali, Myanmar, Nicaragua, Russia, Somalia, South Sudan, Ukraine, Yemen,** and **Zimbabwe.**[5] These sanctions are typically imposed on certain individuals and entities in, or associated with prior or current regimes in, these countries, or involved in illicit activity particularly related to the regime or country. These jurisdictions are generally higher-risk jurisdictions for sanctions compliance.

C. **Sectoral Sanctions.** These sanctions target particular entities within specific sectors of a country's economy. Currently, the primary sectoral sanctions that OFAC imposes relate to the Russia/Ukraine program. Entities subject to Russia- related sectoral sanctions are listed on OFAC's Sectoral Sanctions Identifications ("**SSI**") List. Unlike with persons added to the SDN List, companies may engage in most business with parties on the SSI List, because only certain types of dealings are prohibited. As with SDNs, OFAC considers any entity 50% or more owned in the aggregate by individuals or entities identified on the SSI List to be subject to the same restrictions as SSIs, even if the entity is not itself identified on the SSI List. Any business with an SSI must be approved by the CEO and the Compliance Risk Committee.

The Company will not provide assistance of any kind that would facilitate transactions with sanctioned countries, entities or persons by third parties, including referrals of sales opportunities, approvals, or brokering. In other words, the Company will not assist a third party in performing transactions with sanctioned countries or persons, even if that third party is not legally prohibited from engaging in such transactions.

The Company will not provide any services to or engage in any transactions with countries, regions, entities, or individuals targeted by applicable Sanctions, whether directly or indirectly, unless authorized under all applicable laws.

Any opportunity to engage in transactions with sanctioned jurisdictions or sanctioned persons must be reviewed and approved in advance in writing by the Compliance Risk

[5] The OFAC's country sanctions list can be found here https://ofac.treasury.gov/sanctions-programs-and-country-information.

Committee. The Compliance Risk Committee. will be responsible for ensuring all such transactions are only conducted if permitted under applicable Sanctions.

III. OVERVIEW OF EXPORT CONTROLS

It is also the policy of the Company to comply with all relevant Export Controls maintained by the European Union, the United Kingdom, the United States as well as other jurisdictions where the Company does business.

The European Union controls the export, transit and brokering of dual-use items so the European Union can contribute to international peace and security and prevent the proliferation of Weapons of Mass Destruction ("**WMD**"). Dual-use items are goods, software and technology that can be used for both civilian and military applications. Regulation (EC) No 428/2009 (2017 consolidated version) governs the European Union's export control regime, which includes common export control rules, including a common set of assessment criteria and common types of authorizations (individual, global and general authorizations), a common European Union list of dual-use items, a 'catch-all clause' for non-listed items which could be used, for example, in connection with a WMD program, controls on brokering dual-use items and their transit through the European Union, specific control measures to be introduced by exporters, such as record- keeping and registers, and provisions setting up a network of competent authorities supporting the exchange of information and the consistent implementation and enforcement of controls throughout the European Union.

The United Kingdom provides for export controls with respect to dual-use items (*i.e.*, goods, software and technology that can be used for both civilian and military applications) as well as military items and certain other items, including torture equipment and radioactive sources. The UK dual-use export controls are governed by the EU Dual Use Regulation, which has been transposed into UK law as a "retained" EU law. Items that are subject to export controls are consolidated within the UK Strategic Export Control Lists,[6] which form basis for the determination whether any products, software or technology are 'controlled' and therefore require an export license. If an item is not included on the control lists, a license may still be needed under end-use controls.

The United States administers controls over the export, reexport, and transfer of goods, technology, and software for national security, foreign policy, nuclear non-proliferation, and other policy reasons. The U.S. Department of Commerce, Bureau of Industry and Security ("**BIS**"), has jurisdiction over most (but not all) such exports, re-exports, and

[6] The UK Strategic Export Control Lists are available here https://www.gov.uk/government/publications/uk-strategic-export-control-lists-the-consolidated-list-of-strategic-military-and-dual-use-items-that-require-export-authorisation.

transfers.[7] Among other things, BIS controls dual use items by including them on the Commerce Control List, 15 CFR Part 774. A license from BIS (and/or another U.S. agency), may be required prior to engaging in exports, re-exports, or transfers involving controlled items and a prohibited end use, end destination, or end user.

Prohibited end uses include (but are not limited to) terrorist-related end uses, the development, production, or use of rocket and missile systems, and weapons of mass destruction.

BIS regulations provide that no goods, even if they are not otherwise prohibited for export can be shipped to certain persons (such as for use in terrorist activities, narcotics proliferation, or the proliferation of weapons of mass destruction or chemical and biological weapons), for persons associated with such activities, or to restricted governments or countries/regions. The U.S. Commerce Department Bureau of Industry and Security maintains lists of end-users subject to export restrictions, the Entity List, Denied Party List, and the Unverified List (collectively, "**Prohibited Parties**").

The Company does not currently engage in any exports or reexports of items controlled for purposes of EU, UK or US Export Controls.

Any opportunity to engage in any exports or reexports of items controlled for purposes of EU, UK or US Export Controls must be reviewed and approved in advance in writing by the Company's CEO and the Compliance Risk Committee. The Company's CEO and the Compliance Risk Committee will be responsible for ensuring all such transactions are only conducted if permitted under applicable Export Controls.

In any case where an employee is uncertain as to the applicability of Export Controls to a particular matter, the employee should contact the Compliance Risk Committee to enable a further determination of the applicability of any Export Controls.

IV. IDENTIFYING RED FLAGS

While what is a red flag for a particular transaction will vary by product, market and many other factors, the following are some examples:

- The counterparty has a name or address similar to a sanctioned entity or individual.
- The counterparty or an agent is reluctant to provide normal information about:
    - The counterparty's identity;

[7] The Company does not deal in any defense articles, defense services, or related technical data that are controlled under the International Traffic in Arms Regulations (the "**ITAR**").

- The end use of the product; or
- Whether the product will be re-exported or used domestically.

- The payment terms or method are unusual (such as cash for items not normally sold for cash).
- Shipping or delivery terms are vague or indicate a reshipment is going to take place.
- The counterparty is not familiar with the product or its uses.
- There are suspicious or questionable circumstances involved in a sale, such as a lack of customary information about a proposed transaction, a request to use an unusual route for shipment or unusual product specifications that are inconsistent with the customer's stated end-use of the product.

If a transaction presents any of the red flags listed above, please confirm with the Compliance Risk Committee whether additional diligence is required prior to proceeding with the transaction.

V. COMPLIANCE PROCEDURES

The Company will maintain certain procedures to ensure the Company's compliance with Sanctions and Export Controls. The Company will take steps to ensure that it does not do business or engage in any transactions with countries, regions, entities, or individuals targeted by applicable Sanctions or Export Controls. The Company will also require that those contracts with third parties where, due to their nature, there may be a risk in terms of Sanctions and Export.

Controls (including, but not limited to, all contracts where the Company supplies goods, software or technology) include terms designed to ensure compliance with applicable Sanctions and Export Controls.

In addition, this Policy requires that training be administered to ensure that the appropriate Company employees have the information and skills required to identify Sanctions and Export Controls-related red flags and resolve those red flags in compliance with this Policy. This Policy also dictates that the Company will conduct in-house routine audits of its procedures to ensure ongoing compliance, and records of such audits shall be maintained for a period of five (5) years.

A. Sanctioned Jurisdiction/Restricted Party Screening

New and existing business relationships and new transactions will be screened against

Sanctions and Export Controls Prohibited Party lists maintained by the United Nations, the European Union, the United Kingdom and the United States, as well as for references to comprehensively sanctioned countries or territories (collectively, "**Restricted Parties**").

To prevent dealings with Restricted Parties, the Company conducts Restricted Party screening of all customers, vendors engaged by the Company, and of other new third-party counterparties ("**Counterparty Information**").

1. The screening of new customers, vendors engaged by the Company and of other third-party counterparties (collectively, "**Counterparties**") occurs prior to the Company entering into a business relationship with these entities.

2. The Company conducts this Restricted Party screening manually through a search of the counterparty's name via:

   (a) (for U.S. sanctions) the U.S. government's Consolidated Screening List (https://www.trade.gov/data-visualization/csl-search) with "fuzzy name" enabled;

   (b) (for EU sanctions) the EU's Consolidated List of Persons, Groups and Entities Subject to EU Financial Sanctions (https://data.europa.eu/data/datasets/consolidated-list-of-persons-groups-and- entities-subject-to-eu-financial-sanctions?locale=en);

   (c) (for UK sanctions) the UK government's Sanctions List (https://www.gov.uk/government/publications/the-uk-sanctions-list);

   (d) (for Canadian Sanctions) the Canadian government's Consolidated Canadian Autonomous Sanctions List (https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/consolidated-consolide.aspx?lang=eng); and

   (e) (for UN sanctions) the UN Security Council's Consolidated List (https://www.un.org/securitycouncil/content/un-sc-consolidated-list).

3. Given that the Restricted Party lists frequently change, the Company also conducts re-screening of all its suppliers once before entering into the relevant agreement once per year.

4. Any potential matches identified by this Restricted Party screening are automatically flagged to the Compliance Risk Committee for review.

5. If the screening identifies an exact match of a Counterparty's full name and address to a Restricted Party, the account is immediately and automatically suspended and flagged to the Company's legal department for review.

6. If the screening identifies a potential match between the Counterparty and a Restricted Party, the Company will follow the below procedures for "clearing" those potential matches:

   (a) The Company follows the following guidance to determine whether any "hit" is a valid match:

   Step 1: Compare the Counterparty name with the name on the sanctions list. Is the Counterparty name an individual while the name on the sanctions list is a vessel, organization, or company (or vice versa)?

   - If yes, it is not a valid match.
   - If no, please continue to Step 2 below.

   Step 2: How much of the listed entry's name is matching against the Counterparty? Is just one of two or more names matching (*i.e.*, just the last name), rather than the full name?

   - If yes, it is not a valid match.
   - If no, please continue to Step 3 below.

   Step 3: Compare the complete sanctions list entry with all of the Counterparty Information. Is there additional information that would help the Company to determine whether there is a valid match (*e.g.*, business address, passport number or date of birth for individuals, corporate registration number for corporations)?

   - If yes, go back and get more information regarding the Counterparty and then compare the complete information against the entry.

- If no, please continue to Step 4 below.

Step 4: Are there a number of similarities or exact matches between the sanctions list entry and the Counterparty Information?

- If yes, the Company may not proceed with any business, directly or indirectly, with such third party until the potential match is fully "cleared," which may require reaching out to the applicable Counterparty for additional information.

- If no, it is not a valid match.

(b) If, after following the steps above, the Company is unable to determine whether a match is valid, it should go back to the applicable Counterparty to request additional information in order to make a determination as to the validity of the potential match.

(c) When the Company's business operations team cannot clear or confirm the potential match internally, the Company's business operations team will consult with the Compliance Risk Committee, and as needed, outside counsel with renowned expertise on Sanctions and Export Controls issues.

7. The Company's Compliance Risk Committee is responsible for creating and maintaining records of all screenings conducted and all activities undertaken to "clear" potential matches for a period of five years from the date of such activity. The Company will record such information using the screening software or a similar recordkeeping format.

B. Contracts with Third Parties

The Company requires appropriate Sanctions and Export Control compliance language to be incorporated into its new or amended contracts with customers, vendors, and other third-parties where, due to their nature, there may be a risk in terms of Sanctions and Export Controls (including, but not limited to, all contracts where the Company supplies goods, software or technology). Before entering into a new or amended contract, please confirm with the Company's legal department that appropriate Sanctions and Export Control compliance-related language is included in the contract (if required) or approved by the Counterparty, and obtain the approval in writing.

The following language should be included in relevant third party contracts:

[Counterparty] hereby warrants that it will at all times comply with all applicable regulations and prohibitions administered by the United Nations, the European Union, the

United Kingdom, the United States and other applicable jurisdictions relating to anti-terrorism measures, sanctions, trade embargoes, export and trade controls (including, without limitation, the export controls administered by the European Union and the U.S. Department of Commerce Bureau of Industry), collectively, the "Sanctions", and that neither it, nor any of its subsidiaries nor affiliates, nor any of their respective officers, directors, or employees is currently: (i) included in any restricted party lists pursuant to Sanctions; (ii) organized or located in a comprehensively sanctioned jurisdiction pursuant to Sanctions; (iii) owned fifty percent or more by any persons identified in (i) or (ii); or (iv) involved in any violations, government investigations, or enforcement actions related to Sanctions.

However, it will not be required to include the previous paragraph in the relevant third party contracts, provided that such contracts contain a direct link to a website where the Policy is available.

No variation or removal of this language is permitted without the review and express written approval of the Compliance Risk Committee.

C. Training

1. The Company will distribute this Policy to all employees. The Compliance Risk Committee is responsible for promptly updating the Policy upon any changes to Sanctions and Export Controls and recirculating to employees. The employee certification in Appendix A, signifying that each employee has read, understood, and promised to abide by the Policy, will also be collected from all employees at the time of hire and on a periodic basis thereafter, as well as following any revisions to the Policy. The Compliance Risk Committee will maintain a record of all employee certifications on file for a period of five (5) years from the date of certification.

2. Outside of the formal training process, the Compliance Risk Committee will act as a point of contact for employees to direct Sanctions and Export Controls-related questions in the ordinary course of business.

D. Audits/Risk Assessment

1. The Company will conduct periodic internal audits of its Sanctions and Export Controls compliance procedures to confirm that such procedures are operating correctly and effectively. The auditing will include testing of the Restricted Party screening procedures and screening software and of the country blocking procedures.

2. The Company will also perform spot-check reviews on the addresses of random samplings of its existing list of customers during the audit and confirm that there are no customers in sanctioned countries or who are sanctioned parties.

3. The Company will periodically conduct risk assessments to identify its Sanctions and Export Controls risk and update this Policy, including an assessment of its customers, intermediaries, and Counterparties, the products and services it offers, and the geographic locations in which it operates. As appropriate, this risk assessment will be updated to account for any root causes of any apparent violations or systematic deficiencies identified by the Company, either through the audits or the routine course of business.

VI. ADDITIONAL RESPONSIBILITIES

It is your responsibility to review and comply with policies and procedures and to seek appropriate guidance from the Compliance Risk Committee. Because of the complicated nature of Sanctions and Export Controls, the Compliance Risk Committee is available to discuss any questions or concerns you may have with respect to your compliance obligations. If you learn of conduct that may constitute a violation of Sanctions or Export Controls, you are required to report it immediately to the Compliance Risk Committee. Reports may be made anonymously at the mailbox that is allocated for this purpose at the main office. The Company will not tolerate retaliation of any kind against any individual who in good faith makes inquiries or reports regarding, or participates in external or internal investigations of, a potential violation of this Policy or any applicable Sanctions or Export Controls.

Violations of this Policy will result in appropriate disciplinary actions, up to and including termination of the corresponding employment or commercial agreement. Failure to comply with applicable Sanctions and Export Controls may result in significant criminal, civil, and administrative penalties, including imprisonment and fines.

VII. CONTACTS

If you have any questions or concerns about these procedures, promptly contact the Compliance Risk Committee or the CEO.