



## Code of Ethics and Business Conduct & Anti-Corruption Policies

### A. Code of Ethics and Business Conduct Policy

#### 1. Introduction

1.1 The Board of Directors of Climb Global Solutions, Inc.(together with its subsidiaries, the "**Company**") has adopted this Code of Ethics and Business Conduct (the "**Code**").

- a. promote honest and ethical conduct, including the ethical handling of actual or apparent conflicts of interest;
- b. promote full, fair, accurate, timely and understandable disclosure in reports and documents that the Company files with, or submits to, the Securities and Exchange Commission (the "**SEC**") and in other public communications made by the Company;
- c. promote compliance with applicable governmental laws, rules and regulations;
- d. promote the protection of Company assets, including corporate opportunities and confidential information;
- e. promote fair dealing practices;
- f. deter wrongdoing; and
- g. ensure accountability for adherence to the Code.

1.2 All, officers, directors and employees are required to be familiar with the Code, comply with its provisions and report any suspected violations as described below in Section 10., Reporting and Enforcement.

#### 2. Honest and Ethical Conduct

2.1 The Company's policy is to promote high standards of integrity by conducting its affairs honestly and ethically.

2.2 Each, officer, director and employee must act with integrity and observe the highest ethical standards of business conduct in his or her dealings with the Company's customers, suppliers, partners, service providers, competitors, employees and anyone else with whom he or she has contact in the course of performing his or her job.

#### 3. Conflicts of Interest

3.1 A conflict of interest occurs when an individual's private interest (or the interest of a member of his or her family) interferes, or even appears to interfere, with the interests of the Company as a whole. A conflict of interest can arise when an employee, officer or director (or a member of his or her family) takes actions or has interests that may make it difficult to perform his or her work

for the Company objectively and effectively. Conflicts of interest also arise when an employee, officer or director (or a member of his or her family) receives improper personal benefits as a result of his or her position in the Company.

3.2 Loans by the Company to, or guarantees by the Company of obligations of, employees or their family members are of special concern and could constitute improper personal benefits to the recipients of such loans or guarantees, depending on the facts and circumstances. Loans by the Company to, or guarantees by the Company of obligations of, any director or executive officer or their family members are expressly prohibited.

3.3 Whether or not a conflict of interest exists or will exist can be unclear. Conflicts of interest should be avoided unless specifically authorized as described in Section 3.4.

3.4 Persons other than executive officers and directors and who have questions about a potential conflict of interest or who become aware of an actual or potential conflict should discuss the matter with, and seek a determination and prior authorization or approval from, their supervisor, manager or other appropriate personnel. Supervisors, managers or other appropriate personnel may not authorize or approve conflict of interest matters or make determinations as to whether a problematic conflict of interest exists without first providing the Chief Compliance Officer, who shall be the Chief Financial Officer or other officer designated by the Board, with a written description of the activity and seeking the Chief Compliance Officer's written approval. If the supervisor, manager or other appropriate personnel is himself or herself involved in the potential or actual conflict, the matter should instead be discussed directly with the Chief Compliance Officer.

Executive officers and directors must seek determinations and prior authorizations or approvals of potential conflicts of interest exclusively from the Audit Committee of the Board of Directors (the "Audit Committee").

## 4. Compliance

4.1 Employees, officers and directors should comply, both in letter and spirit, with all applicable laws, rules and regulations in the cities, states and ***countries*** in which the Company operates.

4.2 Although not all employees, officers and directors are expected to know the details of all applicable laws, rules and regulations, it is important to know enough to determine when to seek advice from appropriate personnel. Questions about compliance should be addressed to the Company's legal counsel. Contact information for Company legal counsel is available from the Chief Compliance Officer.

4.3 No, officer, director or employee may purchase or sell any Company securities while in possession of material non-public information regarding the Company, nor may any officer, director or employee purchase or sell another company's securities while in possession of material non-public information regarding that company. All officers, directors and employees must familiarize themselves with and follow the Company's statement of policy regarding compliance with all applicable securities laws and regulations and the avoidance of conflicts of interest ("Insider Trading Policy"). Company policy prohibits and it is illegal for any director, officer or

employee to use material non-public information regarding the Company or any other company to:

- a. obtain profit for himself or herself; or
- b. directly or indirectly "tip" others who might make an investment decision on the basis of that information.

## 5. Disclosure

5.1 The Company's periodic reports and other documents filed with the Securities and Exchange Commission ("SEC"), including all financial statements and other financial information, must comply with applicable federal securities laws and SEC rules.

5.2 Each officer, director and employee who contributes in any way to the preparation or verification of the Company's financial statements and other financial information must ensure that the Company's books, records and accounts are accurately maintained. Each director, officer and employee must cooperate fully with the Company's accounting and internal audit departments, as well as the Company's independent public accountants and legal counsel.

5.3 Each director, officer and employee who is involved in the Company's disclosure process must:

- a. be familiar with and comply with the Company's disclosure controls and procedures and its internal control over financial reporting; and
- b. take all necessary steps to ensure that all filings with the SEC and all other public communications about the financial and business condition of the Company provide full, fair, accurate, timely and understandable disclosure.

## 6. Protection and Proper Use of Company Assets

6.1 All officers, directors and employees should protect the Company's assets and ensure their efficient use. Theft, carelessness and waste have a direct impact on the Company's profitability and are prohibited.

6.2 All Company assets should be used only for legitimate business purposes, though incidental personal use is permitted. Any suspected incident of fraud or theft should be reported for investigation immediately.

6.3 The obligation to protect Company assets includes the Company's proprietary information. Proprietary information includes intellectual property such as trade secrets, patents, trademarks, and copyrights, as well as business and marketing plans, engineering and manufacturing ideas, designs, databases, records and any non-public financial data or reports. Unauthorized use or distribution of this information is prohibited and could also be illegal and result in civil or criminal penalties.

## 7. Corporate Opportunities

All officers, directors and employees owe a duty to the Company to advance its interests when the opportunity arises. Directors, officers and employees are prohibited from taking for themselves

personally (or for the benefit of friends or family members) opportunities that are discovered through the use of Company assets, property, information or position. Officers, directors and employees may not use Company assets, property, information or position for personal gain (including gain of friends or family members). In addition, no director, officer or employee may compete with the Company.

## 8. Confidentiality

Officers, directors and employees should maintain the confidentiality of information entrusted to them by the Company or by its customers, suppliers or partners, except when disclosure is expressly authorized or is required or permitted by law. Confidential information includes all non-public information (regardless of its source) that might be of use to the Company's competitors or harmful to the Company or its customers, suppliers or partners if disclosed. Officers, directors and employees are reminded to comply with the provisions of any confidentiality agreements that they may have entered into with the Company.

## 9. Fair Dealing

Each officer, director and employee must deal fairly with the Company's customers, suppliers, partners, service providers, competitors, employees and anyone else with whom he or she has contact in the course of performing his or her job. No officer, director or employee may take unfair advantage of anyone through manipulation, concealment, abuse or privileged information, misrepresentation of facts or any other unfair dealing practice.

## 10. Reporting and Enforcement

### 10.1 Reporting and Investigation of Violations.

- a. Actions prohibited by this Code involving directors or executive officers must be reported to the Audit Committee.
- b. Actions prohibited by this Code involving anyone other than a director or executive officer must be reported to the reporting person's supervisor, manager or other appropriate personnel.
- c. After receiving a report of an alleged prohibited action, the Audit Committee, the relevant supervisor, manager or other appropriate personnel must promptly take all appropriate actions necessary to investigate. If the allegations involve the relevant manager, supervisor, or the Audit Committee, then the matter must be referred to the chair of the Board of Directors or other appropriate personnel for appropriate actions.
- d. All officers, directors and employees are expected to cooperate in any internal investigation of misconduct.

### 10.2 Enforcement

- a. The Company must ensure prompt and consistent action against violations of this Code.
- b. After investigating a report of an alleged prohibited action by an executive officer or director, the Audit Committee reports its determination whether a violation of this Code has or has not occurred to the Board of Directors.

- c. After investigating a report of an alleged prohibited action by any other person, the relevant supervisor, manager or other appropriate personnel will report its determination whether a violation of this Code has or has not occurred to the Audit Committee.
- d. Upon receipt of a determination that there has been a violation of this Code, the Board of Directors will take such preventative or disciplinary action as it deems appropriate, including, but not limited to, reassignment, demotion, dismissal and, in the event of criminal conduct or other serious violations of the law, notification of appropriate governmental authorities.

### 10.3 Waivers

- a. The Board of Directors may, in its discretion, waive any violation of this Code.
- b. Any waiver for an executive officer or a director shall be disclosed as required by SEC and NASDAQ rules.

### 10.4 Prohibition on Retaliation.

The Company does not tolerate acts of retaliation against any officer, director or employee who makes a good faith report of known or suspected acts of misconduct or other violations of this Code.

## B. Anti-Corruption Policy

### 1. Introduction

**Combating Corruption.** Climb Global Solutions, Inc. (the "**Company**") operates in a wide range of legal and business environments, many of which pose challenges to our ability to conduct our business operations with integrity. As a company, we strive to conduct ourselves according to the highest standards of ethical conduct. Throughout its operations, the Company seeks to avoid even the appearance of impropriety in the actions of its directors, officers, employees, and agents. Accordingly, this Anti-Corruption Policy ("**Policy**") reiterates our commitment to integrity, and explains the specific requirements and prohibitions applicable to our operations under anti-corruption laws, including, but not limited to, the US Foreign Corrupt Practices Act of 1977 ("**FCPA**"), the U.K. Bribery Act (2010 c. 23) ("**UKBA**"), Canada Corruption of Foreign Public Officials Act (S.C. 1998, c. 34) ("**CFPOA**") and the Dutch Criminal Code (articles 177, 178, 328, 363, 364) ("**DCC**") and the laws of any jurisdiction the Company operates in either directly or indirectly, (collectively, the "**Anti-Corruption Laws**"). This Policy contains information intended to reduce the risk of corruption and bribery from occurring in the Company's activities. The Company strictly prohibits all forms of corruption and bribery and will take all necessary steps to ensure that corruption and bribery do not occur in its business activities. Under the FCPA, it is illegal for US persons, including US companies or any companies traded on US exchanges, and their subsidiaries, directors, officers, employees, and agents, to bribe non-US government officials. The UKBA, CFPOA and DCC, as well as the laws of many countries in which the Company operates, also prohibit the bribery of non-government officials as well as (for them) foreign officials, which would include US government officials.

The concept of prohibiting bribery is simple. However, understanding the full scope of the FCPA and the other Anti-Corruption Laws is essential as they directly affect everyday business

interactions between the Company and both US and non-US governments and government- owned or government-controlled entities, as well as other private enterprises wherever in the world they operate. Violations of the FCPA can also result in violations of other US laws, including anti-money laundering, mail and wire fraud, and conspiracy laws and there may be similar consequences in the other jurisdictions noted above. The penalties for violating the FCPA and the other Anti-Corruption Laws are severe. In addition to being subject to the Company's disciplinary policies (including termination), individuals who violate these laws may also be subject to imprisonment and fines. Aside from the reputational damage being connected to bribery would cause, under the UKBA the Company may also be subject to an unlimited fine. This Policy generally sets forth the expectations and requirements for compliance with the FCPA and other Anti-Corruption Laws.

**Applicability.** This Policy is applicable to all of the Company's operations worldwide. This Policy applies to all of the Company's officers, directors and employees. This Policy also applies to the Company's agents, consultants, joint venture partners, and any other third-party representatives that, on behalf of the Company, have conducted, or are likely to conduct, business or otherwise provide services on behalf of the Company or interact with either government officials or commercial counterparties and customers on behalf of the Company.

## 2. Prohibited Payments

Company employees and agents are prohibited from directly or indirectly making, promising, authorizing, or offering anything of value to any person on behalf of the Company to secure an improper advantage, obtain or retain business, or direct business to any other person or entity. This prohibition includes payments to third-parties where the third-party will use any part of the payment for bribes.

Under the UKBA, where the thing of value is directly or indirectly promised, given or offered to a "foreign" (i.e. non-UK) government official, with the intention of influencing the recipient in his capacity as a foreign official in order to obtain or retain business, there is no need to show that the official did anything improper.

- a. **Cash and Non-Cash Payments: "Anything of Value."** Payments that violate the FCPA and Anti-Corruption Laws may arise in a variety of settings and include a broad range of payments beyond the obvious cash bribe or kickback. The FCPA and other Anti-Corruption Laws prohibit giving "anything of value" for an improper purpose. This term is very broad and can include, for example:
  - i. Gifts.
  - ii. Travel, meals, lodging, entertainment, or gift cards.
  - iii. Loans or non-arm's length transactions.
  - iv. Charitable or political donations and sponsorship.
  - v. Business, employment, or investment opportunities.
  - vi. Cryptocurrency.
- b. **Foreign Government Officials.** As set out above, the FCPA is concerned with the bribery of non-US government officials. However, other Anti-Corruption Laws include US government officials as "foreign" officials to whom such payments are prohibited. Who falls within this category is defined broadly in the Anti-Corruption Laws to include:

- i. Officers, representatives and employees of a government or any department, agency, branch or instrumentality thereof, including elected and appointed officials at the federal, state/provincial, and municipal level.
- ii. Officers or employees of a company or business owned in whole or in part by a government (a state owned or controlled enterprises).
- iii. Officers or employees of a public international organization (such as the United Nations, World Bank, or the European Union).
- iv. Political parties or officials thereof.
- v. Candidates for political office.

This term also includes anyone acting on behalf of any of the above and the family members of anyone qualifying as a government or public official.

In terms of application under the FCPA, it is only where the above are non-US officials that there is a prohibition. Similarly, under other Anti-Corruption Laws the officials of the relevant state are not included, e.g. UK officials are not included as foreign officials under the UKBA. However, given the application of multiple Anti-Corruption Laws to the Company, it is likely that any government official being dealt with on behalf of the Company will fall within the definition of a foreign government official under one of the Anti-Corruption Laws and caution must therefore be exercised in those dealings.

On occasion, a government official may attempt to solicit or extort improper payments or anything of value from Company employees or agents. Such employees or agents must inform the government official that the Company does not engage in such conduct and immediately contact the Chief Compliance Officer.

- c. **Commercial Bribery.** Bribery involving commercial (non-governmental parties) is prohibited by many of the Anti-Corruption Laws and is also prohibited under this Policy. To this end, Company employees and agents shall not offer, promise, authorize the payment of, or pay or provide anything of value to any employee, agent, or representative of another company to induce or reward the improper performance of any function or any business-related activity. Company employees and agents also shall not request, agree to receive, or accept anything of value from any employee, agent, or representative of another company or entity as an inducement or reward for the improper performance of any function or business-related activity.

On occasion, a person may attempt to solicit or extort improper payments or anything of value from Company employees or agents. Such employees or agents must inform the person that the Company does not engage in such conduct and immediately contact the Chief Compliance Officer.

### 3. Permitted Payments

The FCPA does not prohibit all payments to non-US government officials. In general, the FCPA permits three categories of payments:

- a. **Facilitating Payments.** The FCPA includes an exception for nominal payments made to low-level government officials to ensure or speed the proper performance of a government official's routine, non-discretionary duties or actions, such as:

- i. Clearing customs.
- ii. Processing governmental papers such as visas, permits, or licenses.
- iii. Providing police protection.
- iv. Providing mail, telephone, or utility services.

The other Anti-Corruption Laws do not contain exemptions for Facilitating Payments and such payments may be considered bribes under the UKBA, CFPOA, DCC and applicable local laws. As set out above, under those laws such payments within the US would also likely be caught. Any requests to make Facilitating Payments must be directed to the Chief Compliance Officer and pre-approved in writing.

- b. **Promotional Hospitality and Marketing Expenses or Pursuant to a Contract.** The Company may pay for the reasonable cost of a non-US government official's meals, lodging, or travel if, and only if, the expenses are bona fide, reasonable, and directly related to the promotion, demonstration, or explanation of Company products or services, or the execution of a contract with a non-US government or agency.
- c. **Promotional Gifts.** Promotional gifts of nominal value may be given to a non-US government official as a courtesy in recognition of services rendered or to promote goodwill. These gifts must be nominal in value and should generally bear the trademark of the Company or one of its products.

Likewise, other Anti-Corruption laws do not prohibit the provision of bona fide and reasonable hospitality and gifts to US or other government officials but these should be limited as above and only provided where strictly necessary. Given there is no requirement to show impropriety on the part of the official for an offence to be committed under the UKBA, extreme caution should be exercised before providing any gifts or hospitality to non-UK officials and pre-approval should be sought from the Chief Compliance Officer.

## 4. Gifts and Hospitality

The FCPA does not address provision of gifts and hospitality to commercial counterparties and customers. However, as noted above, other Anti-Corruption Laws and this Policy prohibit bribery of non-governmental persons and accordingly the use of gifts and hospitality for this purpose.

Normal and appropriate hospitality (given and received) to or from third parties is not prohibited. The Company's policy on providing or offering entertainment, and in giving gifts to third parties, is that: (i) it should be expected to develop the Company's relationship with the recipient and/or the Company's reputation in the market; (ii) the value should be reasonable and proportionate given the nature of the relationship; and (iii) it must not include cash or a cash equivalent (such as gift certificates or vouchers).

The hospitality or gift should be referred to the Chief Compliance Officer for approval if:

- a. The value of the gift exceeds \$250 on any one occasion or \$600 over the course of a year;
- b. The value of the hospitality exceeds \$250 on any one occasion or \$600 over the course of a year;

- c. The recipient is a government official anywhere in the world; or
- d. The hospitality is also being provided to friends or family members of the recipient.

Hospitality and/or gifts must never be given with the intention of influencing a third party to obtain or retain business or a business advantage, or to reward the provision or retention of business or a business advantage, or in explicit or implicit exchange for favors or benefits. It should never be offered if the recipient is expected to have a significant influence in the outcome of a current competitive tendering process.

Accepting personal gifts or hospitality of an extravagant nature from existing or potential competitors, suppliers, partners, intermediaries or agents is also strictly prohibited.

## 5. Political and Charitable Contributions

Contributions made on behalf of the Company (rather than in a personal capacity) to candidates for non-US political office are prohibited unless the Chief Compliance Officer pre-approves them in writing. Charitable contributions made on behalf of the Company (rather than in a personal capacity) to non-US charities must also be pre-approved in writing by the Chief Compliance Officer.

If the intention of the contribution is, or there is, or may be, a perception by any other party, that the contribution is to gain an improper business advantage or to place undue influence on a person responsible for a decision, a service or a contract, then the contribution should not be given.

## 6. Record Keeping

The FCPA further prohibits misrepresenting transactions in the Company's books and records. It is the Company's policy to implement and maintain internal accounting controls based upon sound accounting principles. All accounting entries in the Company's books and records must be timely and accurately recorded and include reasonable detail to fairly reflect transactions. These accounting entries and the supporting documentation must be periodically reviewed to identify and correct discrepancies, errors, and omissions.

- a. **Authorization for Transactions.** All transactions involving the provision of anything of value to a US or non-US government official or commercial counterparty or customer must occur only with appropriate Company authorization.
- b. **Recording Transactions.** All transactions involving the provision of anything of value to a US or non-US government official or commercial counterparty or customer must be recorded in accordance with generally accepted accounting principles.
- c. **Tracking Transactions.** All transactions involving the provision of anything of value to a US or non-US government official or commercial counterparty or customer must be tracked in a separate log or record, with supporting documentation identifying:
  - i. The name and position of the employee requesting and authorizing the transaction.
  - ii. The name and position of the US or non-US government official or commercial counterparty or customer involved in the transaction.
  - iii. A description, including the value, of the payment or provision of anything of value, and where applicable, a description of the Company's products or services being promoted or the relevant contractual provision if the payment was made pursuant to a contract.

## 7. Cash Payments

Cash payments of any kind to a third-party, other than documented petty cash disbursements or other valid and approved payments, are prohibited. Company checks shall not be written to "cash," "bearer," or anyone other than the party entitled to payment except to replenish properly used petty cash funds.

## 8. Representatives

All third-party Company representatives must fully comply with the FCPA and other Anti-Corruption Laws.

## 9. Compliance

Company employees and agents must be familiar with and perform their duties according to the requirements set out in this Policy. Company employees or agents who violate this Policy are subject to disciplinary action, up to and including dismissal. Third-party representatives who violate this Policy may be subject to termination of all commercial relationships with the Company.

To ensure that all Company employees and agents are thoroughly familiar with the provisions of this Policy, the FCPA, and the other Anti-Corruption Laws, the Company shall provide anti-corruption training and resources to those Company employees and agents, as appropriate.

Any Company employee or agent who suspects that this Policy may have been violated must immediately notify the Company as specified in the section entitled "Reporting Policy Violations" below. Any Company employee who, in good faith, reports suspected legal, ethical, or Policy violations will not suffer any adverse consequence for doing so. When in doubt about the appropriateness of any conduct, the Company requires that you seek additional guidance before taking any action that may subject the Company to potential liability under the FCPA or other Anti-Corruption Laws.

## 10. Duty to Cooperate

The Company may at times undertake a more detailed review of certain transactions. As part of these reviews, the Company requires all employees, agents, and third-party representatives to cooperate with the Company, outside legal counsel, outside auditors, or other similar parties. The Company views failure to cooperate in an internal review as a breach of your obligations to the Company, and will deal with this failure severely in accordance with any local laws or regulations.

## 11. Questions About the Policy

If you have any questions relating to this Policy, please contact the Chief Compliance Officer.

## 12. Reporting Policy Violations

To report potential violations of this Policy, immediately notify your supervisor, manager or other appropriate personnel.

### 13. Foreign Based Employees, Partners and Consultants

All of the Company's employees, partners and consultants who conduct business outside of the United States of America are also subject to the Company's Anti Bribery Policy, a copy of which may be obtained from the Chief Compliance Officer as well as all of the local laws, rules and regulations.

## C. Sanctions Policy

### 1. Introduction

- 1.1. Various sanctions programs are maintained by the Office of Foreign Assets Control of the US Department of the Treasury (OFAC), the US Department of State (State), the United Nations Security Council (UN), the European Union (EU), any European Union member state, His Majesty's Treasury of the United Kingdom (UK) and other sanctions authorities where Climb Global Solutions, Inc., and its affiliated entities (collectively, the Company) operates. For example, these programs impose various economic sanctions against countries (*e.g.*, Iran, Cuba, North Korea, Syria, *etc.*), entities and individuals within a country (*e.g.*, Venezuela, Nicaragua, Ukraine/Russia/Belarus, *etc.*), and entities and individuals engaged in specific types of activities, such as terrorist organizations and their members, drug trafficking organizations and their members, and groups and individuals that violate human rights, traffic in weapons of mass destruction, *etc.* Employees, officers and directors should comply, both in letter and spirit, with all such applicable law, rules, and regulations in the locations in which the Company or such person operates, is organized, or is resident.
- 1.2. Although not all employees, officers, and directors are expected to know the details of all applicable laws, rules, and regulations, it is important to know enough to determine when to seek advice from appropriate personnel. The economic sanctions laws are enforced by the imposition of substantial fines (*e.g.*, banks have paid over \$1 billion on more than one occasion) for violations. Questions about compliance should be addressed to the Company's legal counsel. Contact information for Company legal counsel is available from the Chief Compliance Officer.
- 1.3. In the United States, the sanctions programs are administered primarily by OFAC and use the blocking of assets and trade restrictions to accomplish US foreign policy and national security goals. The term "blocking" is another word for "freezing" assets—it is simply a way of controlling targeted property. Title to the blocked property remains with the target, but the exercise of powers and privileges normally associated with ownership is prohibited without authorization from OFAC. Blocking immediately imposes an across-the-board prohibition against transfers or dealings of any kind with regards to the property.
- 1.4. OFAC administers and enforces various types of economic sanctions. Almost every OFAC economic sanctions program is unique. This complexity makes compliance difficult and yet critically important. OFAC regulations apply to all "US persons," which includes citizens and permanent residents (*e.g.*, "green card" holders) wherever located, all individuals, entities, and property located in the United States, companies organized under the laws of a state or territory of the United States, and overseas branches of U.S. companies. Certain sanctions programs, including sanctions on Cuba, include subsidiaries of US companies, wherever located, in the definition of US person.
- 1.5. Compliance is achieved, primarily, by checking all counterparties against the OFAC Specially Designated Nationals List (SDN List), available [online](#). OFAC sanctions programs, generally speaking, prohibit any US person (including entities, citizens, permanent residents, or anyone in the United States) from conducting any business with any person or

company on the SDN List and require that any property owned or controlled by an SDN that comes within the custody or control of a US person be blocked and reported to OFAC.

1.6. OFAC sanctions prohibit also “facilitation,” which is an action that may promote or support any transaction by a foreign person that would otherwise be prohibited if performed by a US person. OFAC has broadly interpreted this rule to regulate a US parent company’s interaction with its foreign subsidiaries concerning dealings with target countries or with sanctioned groups or individuals. The OFAC requirements apply to any Company directors, officers or employees who are US persons, even if they are located outside of the United States or work for Company entities that are not US-incorporated companies. US persons may not engage in any activity that facilitates, approves, or supports any transactions by others with designated countries, individuals, or groups. As this restriction extends to US persons, including officers or board members for any of the Company’s entities that operate outside of the United States, any US persons must recuse themselves from board deliberations regarding any agenda items addressing transactions involving sanctioned countries and record their recusals in the board minutes.

1.7. Sanctions laws change frequently, are complicated, and the application of requirements to every possible transaction cannot be summarized succinctly. For these reasons, any questions about sanctions and how they may affect the Company’s business should be addressed to the Company’s legal counsel.

## 2. Countries, Individuals, and Groups Subject to U.S. Sanctions

2.1. OFAC administers and enforces many different economic sanctions programs. Sanctions are a crucial element of the U.S. government’s response to national security and foreign policy concerns such as international terrorism, regional destabilization, human rights abuses, drug trafficking, and repression of democracy. OFAC sanctions are generally understood to include three kinds of programs:

- Comprehensive Sanctions—broadly prohibit US persons from engaging in any transactions involving the government of, and entities owned or controlled by, a sanctioned country. US persons are expected to know the countries subject to OFAC’s comprehensive sanctions (Crimea region of Ukraine, Cuba, Iran, North Korea, and Syria). Some individuals and entities from these countries, and a host of other entities, ships, properties and individuals are identified on OFAC’s Specially Designated Nationals’ List (“SDN List”). These sanctions are also applied against political or drug-trafficking organizations as List-Based Sanctions (explained below).
- List-Based Sanctions—list-based Sanctions prohibit a U.S. person from engaging in transactions involving entities and persons on the SDN List. Typically, these are organizations and their members, such as Hezbollah (the terrorist organization) and Hezbollah officials and members (individuals). Another example are drug cartels and their front companies and members, such as the Cali (Colombia) cartel and the over 100 companies and hundreds of individuals associated with it that are on the SDN List.

- Secondary Sanctions—secondary sanctions are programs that place non-US persons on the SDN List or other list maintained by OFAC for engaging in activities with SDNs that are prohibited to US persons. Persons subject to secondary sanctions are, generally speaking, blocked from doing business in the United States or with US persons. The purpose of secondary sanctions is to increase the impact of US-imposed sanctions.

2.2.Comprehensive Sanctions. At present, comprehensive sanctions exist against the governments of the Crimea region of Ukraine, Cuba, Iran, North Korea, and Syria. Each of the current comprehensive sanctions programs is different in substance but shares certain common features: unlicensed exports of most goods, technologies, and services from the United States to the sanctioned destination (either directly or knowingly via third countries) are prohibited, as are unlicensed imports of any goods, technologies, or services from the sanctioned region into the United States (either directly or knowingly via third countries). OFAC sanctions also prohibit most other commercial and financial transactions with the governments and persons ordinarily resident in these sanctioned countries. Transactions attempting to evade OFAC’s programs are increasingly being discovered and penalized by OFAC or the U.S. Department of Justice, such as sales of a US product from third-country inventory to an entity in a blocked country. For this reason, any flow of a US company’s goods to a comprehensive sanction country should raise a red flag and be reviewed by Company’s legal counsel.

2.3.List-Based Sanctions. OFAC’s List-Based Sanctions vary in scope. These programs may be tied to a certain country or region or target certain activities, such as opposing democracy or the rule of law, terrorist activities, drug trafficking, cyber-crimes, or human rights violations. For example, OFAC sanctions on Somalia do not broadly prohibit transactions with Somalia. Rather they address transactions with certain designated persons, including those engaged in acts that directly or indirectly threaten the peace, security, or stability of Somalia. Similarly, sanctions imposed against Belarus and Russia related to the invasion of Ukraine do not broadly prohibit transactions with those countries but rather address transactions with certain designated persons, including those responsible for or complicit in actions or policies that undermine democratic processes or institutions in Ukraine, threaten the peace, security stability, sovereignty, or territorial integrity of Ukraine, or misappropriate the state assets of Ukraine or of an economically significant entity in Ukraine.

2.4.Secondary Sanctions. Secondary sanctions are sanctions that target non-U.S. persons that engage in certain transactions with sanctioned individuals or entities, operate in proscribed sectors of a sanctioned country’s economy, or engage in prohibited conduct. For instance, under secondary sanctions, a non-US person may be designated as an SDN if it operates in Iran’s shipping sector or conducts transactions with SDNs in Iran (such as listed Iranian banks). Whether secondary sanctions may be imposed depends upon the language of each particular sanctions program. For instance, Ukraine/Russia-related sanctions allow the imposition of secondary sanctions with regard to particular transactions with SDNs designated under that program. Secondary sanctions are often constructed to deter sanctions evasion, penalizing those that facilitate sanctions avoidance or that provide alternative access to finance. For this reason, just because secondary sanctions *may* be imposed does not mean that they *will be*. These sanctions are seen as overreaching by most other countries and, as a

result, are applied more readily by the U.S. to entities in some countries (such as China) than others (such as the United Kingdom) regardless of whether the conduct is similar. Additionally, OFAC maintains also a separate list identifying persons operating in sectors of the Russian economy, called the Sectoral Sanctions Identifications List (“**SSI List**”).

### 3. Summary of OFAC Sanctions Programs as of May 1, 2023

3.1. An alphabetical listing of the sanction programs is set out below:

- **Balkans** (Blocks property of persons threatening stabilization efforts.)
- **Belarus** (Blocks property of persons that undermine Belarus’ democratic processes or institutions.)
- **Burma** (Myanmar) (Blocks property of persons who directly or indirectly threaten the peace, security or stability of the country or commit human rights abuses in Burma.)
- **Burundi** (Blocks property of persons contributing to instability in Burundi.)
- **Central African Republic** (Blocks property of persons contributing to conflict in the Central African Republic.)
- **Counter Narcotics Trafficking Sanctions** (Blocks the property of persons engaged in narcotics trafficking.)
- **Counter Terrorism Sanctions** (Blocks the property of persons engaged in international terrorism activities.)
- **Cuba** (Prohibits most imports from, and most exports to, Cuba either directly or through third countries and the provision of financial and other services to Cuba or nationals of Cuba, unless certain limited authorizations apply.)
- **Cyber Sanctions** (Blocks the property of persons engaged in cybercrimes and related activities.)
- **Democratic Republic of the Congo** (Blocks property of political or military leaders of Congolese or foreign armed groups operating in the DRC that impede the disarmament, repatriation, or resettlement of combatants, recruit or use children in armed conflict, or supply arms in violation of the United Nations arms embargo on the DRC.)
- **Foreign Interference in a U.S. Election Sanctions** (Blocks property of foreign individuals who engaged, directly or indirectly, in activity with the intent of interfering in a U.S. election.)
- **Global Magnitsky Act** (Blocks property of persons involved in serious human rights abuse or corruption in Russia and elsewhere.)
- **Iran** (Prohibits most imports from, and most exports, to Iran either directly or knowingly through third countries and the provision of financial and other services directly or indirectly to Iran or persons ordinarily resident in Iran. Certain limited authorizations may apply, as described in detail below.)
- **Iraq** (Blocks property and property interests of certain persons associated with the former Iraqi regime.)

- **Lebanon** (Blocks property of persons that undermine the sovereignty of Lebanon or its democratic processes and institutions.)
- **Libya** (Blocks the property of certain designated persons and entities in Libya and maintains certain prohibitions on financial transactions with Libya.)
- **Mali** (Blocks property of persons undermining democratic processes in Mali, obstructing the peace process or delivery of humanitarian assistance, trafficking in illegal narcotics, trafficking in persons or otherwise violating human rights.)
- **Nicaragua** (Blocks property of persons undermining democratic institutions and the rule of law.)
- **Non-Proliferation Sanctions** (Blocks the property of proliferators of weapons of mass destruction.)
- **North Korea** (Blocks property of certain designated persons, including those who facilitate North Korean trafficking in arms and related materiel or engage in money laundering, counterfeiting, bulk cash smuggling, and narcotics trafficking. The sanctions also block the unlicensed importation of goods, services and technology from North Korea.)
- **Russia** (Blocks certain dealings in Russian sovereign debt and targets technology companies that support the Russian Intelligence Services' efforts to carry out malicious cyber activities against the United States.)
- **Somalia** (Blocks property of designated persons and entities that engage in acts that threaten the peace, security, or stability of Somalia.)
- **Sudan** (Bans most unlicensed imports from, and unlicensed exports to, Sudan either directly or knowingly through third countries and prohibits most financial dealings with Sudan.)
- **South Sudan** (Blocks the property of persons engaged in activities that threaten peace and security in South Sudan.)
- **Syria** (Blocks property of designated persons, including senior officials of the Syrian government, persons responsible for the commission of human rights abuses in Syria, and persons that have operated, sold or leased information and communications technology that facilitates computer or network disruption, monitoring or tracking that could assist in human rights abuses by the Syrian government. Proscribes specific types of transactions, exports to, and imports from Syria and prohibits new investment in Syria by U.S. persons, the exportation or re-exportation, sale or supply of services to Syria by such persons, and the importation of petroleum products of Syrian origin.)
- **Transnational Criminal Organizations** (Blocks property of designated individuals and entities determined to be significant transnational criminal organizations or to have provided support for, or to be owned or controlled by, or to have acted on behalf of, such organizations.)
- **Ukraine/Russia** (Blocks the property of various Ukrainian and Russian persons involved in destabilizing regional activities. Imposes an embargo on the region of Crimea. Prohibits transactions involving new "debt" and "equity" of various Russian firms in the energy, defense, and financial services sector; prohibits exports of certain equipment to the oil and defense sectors. Since Russia's invasion of Ukraine in February 2022, US sanctions target

Russian government assets, international trade, broad economic sectors, and specific individuals and entities.)

- **Venezuela** (Blocks the property of persons undermining democratic processes in Venezuela.)
- **Yemen** (Blocks property of designated persons that have engaged in acts that directly or indirectly threaten the peace, security, or stability of Yemen.)
- **Zimbabwe** (Blocks property of persons undermining democratic processes or institutions in Zimbabwe.)

#### 4. Specially Designated Nationals

- 4.1. Persons OFAC designates pursuant to its many sanctions programs (see above list) are captured, together with identifying information, generally on the SDN List. US persons are broadly prohibited from engaging in transactions involving SDNs.
- 4.2. SDNs comprise an ever-growing list of thousands of individuals and entities, such as terrorists, narcotics traffickers, or human rights violators that act contrary to U.S. foreign policy objectives. These designations are published on a frequently changing SDN List. The SDN List is maintained on OFAC's website and updated regularly.
- 4.3. If an entity on the SDN List owns, directly or indirectly, whether individually or in the aggregate, a 50 percent or more interest in another entity, that other entity should be considered to be on the SDN List and its property and interests are blocked. This is known as the "**50 Percent Rule**." For example, if Blocked Person X owns 25 percent of Entity A, and Blocked Person Y owns another 25 percent of Entity A, Entity A is deemed also to be an SDN and is blocked.
- 4.4. The SSI List is not part of the SDN List. However, individuals and companies on the SSI List may also appear on the SDN List. Directives found within the SSI List describe prohibitions on dealings with the persons identified.

#### 5. Due Diligence & "Red Flags"

- 5.1 A person violates U.S. sanctions if the person engages in a transaction with knowledge or "reason to know" a violation of U.S. sanctions will occur. Actual knowledge that a transaction involves or will benefit a sanctioned country or SDN is not required for OFAC to find a violation.
- 5.2 It is important for all Company employees to monitor for "red flags" (that is, suspicious circumstances). All Company employees must conduct a reasonable level of due diligence before proceeding with a transaction to ascertain whether a violation of U.S. economic sanctions is likely to occur. At a minimum, all vendors, customers, financial institutions, and other business partners should be screened against the SDN List and any propriety lists to which legal counsel has access.

5.2.1 Examples of "red flags" that should be monitored include the following:

- The customer's name or address is similar to one found on the SDN List.

- The customer or purchasing agent is reluctant to offer information about the end-use or end user of the item.
- The product's capabilities do not fit the buyer's line of business, such as an order for sophisticated computers for a small bakery.
- The item ordered is incompatible with the technical level of the country to which it is being shipped, such as semiconductor manufacturing equipment being shipped to a country that has no electronics industry.
- The customer is willing to pay cash for a very expensive item when the terms of sale would normally call for financing.
- The customer has little or no business background.
- The customer is unfamiliar with the product's performance characteristics but still wants the product.
- Routine installation, training, or maintenance services are declined by the customer.
- Delivery dates are vague, or deliveries are planned for out-of-the-way destinations.
- A freight forwarding firm is listed as the product's final destination.
- The shipping route is abnormal for the product and destination.
- Packaging is inconsistent with the stated method of shipment or destination.
- When questioned, the buyer is evasive and unclear about whether the purchased product is for domestic use, for export, or for reexport.

## 6. Recordkeeping

6.1. OFAC requires US persons to maintain records of transactions subject to OFAC's jurisdiction for a period of 5 years. Records to be maintained include invoices, purchase orders, correspondence, shipping documents, and other transactional documents. Failure to maintain records can form an independent basis for assessing penalties.

## 7. Specific Guidelines for Our Business

- 7.1.Prohibition on Transactions involving the Crimea Region of Ukraine, Cuba, Iran, North Korea, and Syria**—it is the Company’s global policy not to engage in transactions, either directly or indirectly, involving any country or region subject to comprehensive sanctions, including the Crimea regions of Ukraine, Cuba, Iran, North Korea, and Syria.
- 7.2.Prohibition against Transactions with SDNs**—it is the Company’s global policy not to engage in transactions, directly or indirectly, involving any SDN.
- 7.3.Recordkeeping**—it is the Company’s global policy to retain transaction records for five years from the date of the transaction.
- 7.4.Company Screening Policy**—it is the Company’s policy to screen all customers, vendors, suppliers, contractors, and other business partners against the SDN List and SSI List. Furthermore, all business partners located in the following regions should be referred to the Company’s legal counsel for additional screening and approval.

Afghanistan	Haiti
Armenia	Iraq
Azerbaijan	Kazakhstan
Bahrain	Kuwait
Belarus	Kyrgyzstan
Burma	Laos
Cambodia	Lebanon
Central African Republic	Libya
China (PRC)/Hong Kong	Nicaragua
Democratic Republic of Congo	Russia
Egypt	Ukraine
Eritrea	
Georgia	Any Country or Region Listed in 7.1, above

- 7.5.Humanitarian Assistance**—every sanctions program has exceptions allowing humanitarian assistance and informational materials to be sent to the embargoed country or area. Compliance with the humanitarian exception has become substantially more difficult due to additional reporting rules imposed in late 2019. Before engaging in any humanitarian activity, please contact the Company’s legal counsel.

## 8. Decision Tree

- 8.1.See Appendix 1 for a decision tree on the US sanctions process.

## Appendix 1 to Sanctions Policy—US Decision Tree

The Company must **NOT** engage in any transactions involving comprehensive sanctions or blocked entities (i.e., those on the SDN List or SSI List)

This includes executing contracts or using the US financial system for any such transaction

When there is a question or concern about whether a particular activity complies with applicable sanctions laws and regulations, **STOP** and seek guidance from Company legal counsel

