



**SEVEN SEAS WATER GROUP**

Water-as-a-Service®

# Code of Business Conduct & Ethics

---

Effective December 2020  
Revised: December 2020

**SEVEN SEAS WATER**  
**CODE OF BUSINESS CONDUCT AND ETHICS**

**INTRODUCTION**

This *Code of Business Conduct and Ethics* (hereinafter referred to as the “Code”) is intended to provide all of us at Seven Seas Water<sup>1</sup>, with clear standards of business conduct and ethics, as well as to aid us in making ethical and legal decisions when conducting business and performing day-to-day duties for the Company. We expect all our employees to adhere to these standards set forth in the Code, and they apply to all employees, agents, representatives, and suppliers of the Company (“Company Person(s)”), including: (i) full and part-time employees of the Company, (ii) each member of the Company’s executive team, (iii) and each member of the governing board of each entity within the Company. Each employee must acknowledge review of, and agreement to comply with, the Code on an annual basis as a condition of employment with the Company (*see* form attached as Appendix A).

This Code has been approved by the Board of Directors of the Company and may not be modified, amended or restated without the approval of the respective Boards.<sup>2</sup>

The Code is not intended to address every potential situation that may arise. Employees encountering situations that are not addressed specifically in this Code, should always exercise sound judgment, seek advice when appropriate and adhere to the highest ethical standards.

**REPORTING VIOLATIONS UNDER THE CODE**

If any violation, or suspected violation, of the Code is known to a Company Person, he or she has a responsibility, and is required, to report such violations using one or more of the following reporting mechanisms<sup>3</sup>: (i) reporting through the supervisory chain; (ii) contacting the Chief Compliance Officer or the Human Resources Director; (iii) contacting a member of the governing board of either entity within the Company; and (iv) reporting through the Whistleblowing Hotline via telephone for U.S.-based Company Persons at 1-844-279-8283 (the telephone number for non U.S. Company Persons can be found on the following dedicated internet address) or online at: <https://secure.ethicspoint.com/domain/media/en/gui/41684/index.html>

Any Company Person having any information or knowledge regarding the existence of any violation or suspected violation of the Code (including, but not limited to, any of the reportable concerns listed in the *Seven Seas Water Whistleblower Policy*)

---

<sup>1</sup> “Seven Seas Water” means Seven Seas Water Corporation, AUC Group, LLC, Bluefin Water Solutions LLC, Marlin Water Solutions Co, Yellowfin Water Solutions Co., and Tarpon Water Solutions Ltd, as well as their respective affiliates and subsidiaries. Also referred to herein as the “Company”.

<sup>2</sup> This is not an employment contract and does not impact or effect the at-will status of any employee.

<sup>3</sup> *See also* the reporting mechanisms set forth in the *Seven Seas Water Whistleblower Policy* that is attached hereto as Appendix B)

has a duty to report the violation or suspected violation using the Reporting Mechanisms described above. Company Persons' reports made to the Whistleblowing Hotline will be provided directly to the Chief Compliance Officer, HR Director and to a member of the Boards on an anonymous and confidential basis.

Failure to report suspected or actual violations is itself a violation of the Code and may subject the Company Person to disciplinary action, up to and including termination of employment (or other relationship) with the Company or legal action. Reports may be made on a completely confidential and anonymous basis. To the extent any investigation is necessitated by a report, the Company will endeavor to keep the proceedings and the identity of the reporting Company Person confidential to the fullest extent permitted by applicable law.

### **ANTI-RETALIATION PLEDGE**

Any Company Person who in good faith reports a violation or suspected violation under the Code, or any of the reportable concerns listed in the Company's *Whistleblower Policy*, by the Company, or its agents acting on behalf of the Company, or who in good faith raises issues or concerns regarding the Company's business or operations, using the Reporting Mechanisms, will not be at risk of losing his or her position, nor will he or she suffer any form of detrimental action as a result of his or her reporting – even if the violation is not substantiated in a subsequent investigation.

### **COMPLYING WITH THE CODE**

The ultimate responsibility for maintaining our Code rests with each of us. As individuals of personal integrity, we can do no less than to behave in a way that will continue to bring benefit to our Company and ourselves. Applying these standards to our business and work activities is an extension of the values by which we are known as individuals and by which we want to be known as a Company. It is our responsibility to conduct ourselves in an ethical business manner and also to ensure that others do the same. All employees must read and acknowledge the Code annually, which underscores our values and our commitment to ensuring a workplace that includes equal opportunity, dignity and respect, including with respect to our suppliers, affiliates and partners. Violations of the Code may result in a disciplinary response, up to and including termination of any employment (or other relationship) with the Company, and potentially other legal action.

While it is impossible for this Code to describe every situation that may arise, the standards explained in this Code are guidelines to govern our conduct at all times. If you are confronted with situations not covered by this Code, or have questions regarding the matters that are addressed in the Code, you are urged to consult with the Chief Compliance Officer or Human Resources Department. Furthermore, the policies set forth in this Code are in addition to other legal and contractual obligations to the Company and other policies of the Company that Company Persons must comply with, including those set forth in the Company's *Employee Handbook*. Copies of these other policies are available from the Company's Human Resources Department or on the

Company's internal drive. The provisions set out in this Code are not intended to limit or reduce the requirements of any applicable law, regulation or rule. This Code should be viewed as the minimum standards that the Company expects from the Company Persons in the conduct of the Company's business.

## TABLE OF CONTENTS

I.	IMPLEMENTATION OF THE CODE.....	1
II.	GENERAL REQUIREMENTS .....	3
III.	CONFLICTS OF INTEREST .....	3
IV.	PROTECTION AND PROPER USE OF COMPANY ASSETS .....	4
	A. Proper Use of Company Property .....	5
	B. Confidential Information.....	5
	C. Accurate Records and Reporting .....	6
	D. Document Management and Retention .....	6
	E. Corporate Advances .....	7
V.	FAIR DEALING WITH CUSTOMERS, SUPPLIERS, COMPETITORS, AND EMPLOYEES .....	7
	A. Giving Gifts.....	7
	B. Receiving Gifts .....	8
	C. Unfair Competition.....	8
	D. Antitrust Concerns .....	9
	E. Unfair Practices in International Business .....	10
	F. Human Trafficking .....	11
VI.	GOVERNMENT RELATIONS.....	11
	A. Government Procurement .....	11
	B. Payments to Officials.....	12
	C. Political Contributions.....	12
VII.	COMPLIANCE WITH LAWS, RULES AND REGULATIONS.....	12
	A. Equal Employment Opportunity .....	12
	B. Sexual Harassment Policy.....	12
	C. Health, Safety & Environment Laws.....	14
VIII.	QUESTIONS UNDER THE CODE AND WAIVER PROCEDURES .....	14
IX.	FREQUENTLY ASKED QUESTIONS AND ANSWERS.....	15

### APPENDICES

APPENDIX A – COMPANY PERSON’S AGREEMENT TO COMPLY

APPENDIX B – WHISTLEBLOWER POLICY

APPENDIX C – ANTI-CORRUPTION AND TRADE CONTROLS  
COMPLIANCE POLICY

## **I. IMPLEMENTATION OF THE CODE**

The following questions and answers address the Company's implementation of the Code. The procedures are intended to provide confidentiality, anonymity, and, most importantly, freedom from the fear of retaliation when complying with and reporting violations under the Code.

### **Q: Who is responsible for administering, updating and enforcing the Code?**

**A:** The Boards have appointed a Chief Compliance Officer to administer, update and enforce the Code. The Chief Compliance Officer has overall responsibility for overseeing the implementation of the Code. Specific responsibilities of the position are to:

- Develop the Code based on legal requirements, regulations and ethical considerations that are raised concerning Company operations;
- Ensure that the Code is distributed to all employees and that all employees are aware of, understand and acknowledge the principles of the Code;
- Work with the Company's respective Boards to provide a reporting mechanism so that Company Persons have confidential and anonymous methods of reporting not only suspected violations of the Code but concerns regarding federal securities or antifraud laws, accounting issues, or any federal law relating to fraud against shareholders;
- Develop internal procedures designed to monitor and audit compliance with the Code;
- Conduct internal investigations, with the assistance of counsel as needed, of suspected compliance violations;
- Evaluate disciplinary action for Company Persons who violate the Code, and in the case of more severe violations of the Code, make recommendations regarding disciplinary action to the respective Boards or a committee thereof;
- Serve as a point person for reporting violations and addressing questions about the Code;
- Maintain a log of all reports under the Reporting Mechanisms and provide this log to the respective Boards for their review at regular intervals;
- Evaluate the effectiveness of the Code and improve the Code; and
- Revise and update the Code as necessary.

The Chief Compliance Officer may assign a representative from the Human Resources Department or other Company Person to assist with administering, updating and enforcing the Code.

The Chief Compliance Officer will provide a summary of significant matters considered under the Code to the Boards or a committee thereof at each regular meeting thereof or sooner if warranted by the severity of the matter. All proceedings and the identity of the person reporting will be kept confidential to the extent permitted by applicable law.

**Q: If I am aware of a violation of this Code, or suspect such a violation, am I obligated to report it as set forth in this Code?**

**A:** Yes, every Company Person has the responsibility to ask questions, seek guidance, report known and suspected violations and express concerns regarding compliance with this Code or any of the Company's other policies. Anyone who has a reasonable basis to believe that any other Company Person has engaged, or is engaging, in conduct that violates any applicable law, regulations, rules or this Code should promptly report such information as set forth herein.

**Q: How can I contact the Chief Compliance Officer and respective Boards?**

**A:** Reports may be made by telephone, in person, or in writing (by mail to the Company's address, by email or hand delivery) to the Chief Compliance Officer, Human Resources Director or members of the Boards. Any one of these individuals can assist you in answering questions or reporting violations or suspected violations under the Code. The Chief Compliance Officer and a member of the Boards may change from time to time. The Human Resources department can provide the contact information for the Chief Compliance Officer and Board members.

Individuals are encouraged, but not required, to leave a name or and contact number when submitting a report. Such information will facilitate a more thorough investigation. The Chief Compliance Officer and member of the Boards will strive to maintain the integrity and confidentiality of all compliance- related communications. However, in certain circumstances, the identity of the person raising the issue may become known or need to be revealed, particularly if federal, state, local or foreign enforcement authorities become involved in the investigation. The Company cannot guarantee confidentiality when material evidence of a violation of the law is disclosed or if the person is identified during the normal course of an investigation.

**Q: How can I report any concerns that I have in a confidential and anonymous manner?**

**A:** *You may make such reports on a completely anonymous and confidential basis through the Whistleblowing Hotline.* As specified in the attached *Seven Seas Water Whistleblower Policy*, Company Persons may report to this service any concerns a Company Person may have with respect to the Company, including, but not limited to,

concerns with the Company's business or operations, suspected violations of the Code, violations of any applicable law, regulation or rule, or any other issue concerning the Company and their relationship with the Company. Reports made to the Whistleblowing Hotline will be provided directly to the Chief Compliance Officer, the Human Resources Director, and a member of the Boards on an anonymous and confidential basis.

## **II. GENERAL REQUIREMENTS**

Each Company Person is expected to be honest, fair, and accountable in all business dealings and obligations, and to ensure:

- the ethical handling of conflicts of interest between personal and professional relationships and
- compliance with applicable laws, rules and regulations.

## **III. CONFLICTS OF INTEREST**

Company Persons should avoid any situation that may involve, or even appear to involve, a conflict between their personal interests and the interests of the Company. In dealings with current or potential customers, suppliers, contractors, and competitors, each Company Person should act in the best interests of the Company to the exclusion of personal advantage. For purposes of this section, a "competitor" of the Company shall be deemed to be any entity selling or producing products or providing services that are similar to the Company's products or services. Company Persons are prohibited from any of the following activities, which could represent an actual or perceived conflict of interest:

- No Company Person or immediate family member (including any person with whom a Company Person has any relationship by blood, marriage, or adoption, not more remote than first cousin) of a Company Person shall have a significant financial interest in, or obligation to, any third party which does or seeks to do business with the Company or which is an actual or potential competitor of the Company, without prior approval of Chief Compliance Officer, or in the case of executive officers or members of any Board, such Board or a committee thereof; provided, however, that this provision shall not prevent any Company Person from investing in any mutual fund or owning up to 1% of the outstanding stock of any publicly traded company.
- No Company Person shall conduct a significant amount of business on the Company's behalf with a third party which does or seeks to do business with the Company if an immediate family member of the Company Person is a principal or officer of such third party, or an employee of such third party who will play a significant role in the business done or to be done between the Company and such third party, without prior approval of the Chief Compliance Officer, or in the case of executive officers or members of any Board, such Board or a committee thereof.

- No executive officer or employee, or an immediate family member of an executive officer or an employee, shall serve as a director, officer or in any other management or consulting capacity of any competitor of the Company, without the prior approval of the respective Board or a committee thereof.
- No director, or an immediate family member of a director, shall serve as a director, officer or in any other management or consulting capacity of any actual competitor of the Company, without the prior approval of the relevant full Board of Directors or a committee thereof.
- No Company Person shall use any Company property or information or his or her position at the Company for personal gain.
- No Company Person shall engage in activities that are directly competitive with those in which the Company is engaged.
- No Company Person shall divert a business opportunity from the Company to such individual's own benefit. If a Company Person becomes aware of an opportunity to acquire or profit from a business opportunity or investment in which the Company is or may become involved or in which the Company may have an existing or potential interest, the Company Person should disclose the relevant facts to the Chief Compliance Officer. The Company Person may proceed to take advantage of such opportunity only if the Company is unwilling or unable to take advantage of such opportunity as notified in writing by the Chief Compliance Officer.
- No Company Person or immediate family member of a Company Person shall receive any loan or advance from the Company, or be the beneficiary of a guarantee by the Company of a loan or advance from a third party, except for customary advances or corporate credit in the ordinary course of business or approved by the Chief Compliance Officer. Please see the section on "Corporate Advances" below for more information on permitted corporate advances.

Each Company Person should make prompt and full disclosure in writing to the Chief Compliance Officer of any situation that may involve a conflict of interest. Failure to disclose any actual or perceived conflict of interest is a violation of the Code.

#### **IV. PROTECTION AND PROPER USE OF COMPANY ASSETS**

Proper protection and use of Company assets and assets entrusted to it by others, including proprietary information, is a fundamental responsibility of each Company Person. Company Persons must comply with security programs to safeguard such assets against unauthorized use or removal, as well as against loss by criminal act or breach of trust. The provisions hereof relating to protection of the Company's property also apply to property of others entrusted to it (including proprietary and confidential information).

## **A. Proper Use of Company Property**

Company Persons must be good custodians of any Company property that is under their control and use. The removal from the Company's facilities of the Company's property is prohibited, unless authorized by the Company. This applies to furnishings, equipment, and supplies, as well as property created or obtained by the Company for its exclusive use – such as client lists, files, personnel information, reference materials and reports, computer software, data processing programs and data bases. Neither originals nor copies of these materials may be removed from the Company's premises or used for purposes other than the Company's business without prior written authorization from the Company.

The Company's products and services are its property; contributions made by any Company Person to their development and implementation are the Company's property and remain the Company's property even after any relationship with the Company terminates.

Each Company Person has an obligation to use the time for which he or she receives compensation from the Company productively. Work hours should be devoted to activities directly related to the Company's business.

Company Persons must immediately return all Company property—including, without limitation, computer equipment, software, keys and access cards, credit cards, files and any documents (including computerized data and any copies made of any computerized data or software) containing information concerning the Company, its business or its business relationships—to the Company upon termination of employment (or other relationship).

## **B. Confidential Information**

The Company provides its personnel and agents with confidential information relating to the Company and its business with the understanding that such information is to be held in confidence and not communicated to anyone who is not authorized to see it, except as may be required by law. Some examples of information that each Company Person must safeguard include (but are not limited to): the Company's plans and business strategy, unannounced products and/or contracts, sales data, significant projects, technical designs and information, customer and supplier lists, patents, patent applications, trade secrets, manufacturing techniques and sensitive financial or operational information, whether in electronic or paper format. These are costly, valuable resources developed for the exclusive benefit of the Company. No Company Person shall disclose the Company's confidential information to an unauthorized third party or use the Company's confidential information for his or her own personal or another person's benefit. This also applies to information relating to any other person, including the Company's customers or suppliers, obtained during the Company Person's relationship with the Company.

### **C. Accurate Records and Reporting**

In accordance with applicable law, regulations and rule, the Company is required to keep books, records and accounts that accurately and fairly reflect all transactions, dispositions of assets and other events that are the subject of specific regulatory record keeping requirements, including generally accepted accounting principles and other applicable rules, regulations and criteria for preparing financial statements and for preparing periodic reports. All Company reports, accounting records, sales reports, expense accounts, invoices, purchase orders, and other documents must accurately and clearly represent the relevant facts and the true nature of transactions. Reports and other documents should state all material facts of a transaction and not omit any information that would be relevant in interpreting such report or document. Under no circumstance may there be any unrecorded liability or fund of the Company, regardless of the purposes for which the liability or fund may have been intended, or any improper or inaccurate entry knowingly made on the books or records of the Company. No payment on behalf of the Company may be approved or made with the intention, understanding or awareness that any part of the payment is to be used for any purpose other than that described by the documentation supporting the payment. In addition, intentional accounting misclassifications (e.g., expense versus capital) and improper acceleration or deferrals of expenses or revenues are unacceptable reporting practices that are expressly prohibited.

The Company has developed and maintains a system of internal controls to provide reasonable assurance that transactions are executed in accordance with management's authorization, are properly recorded and posted, and in compliance with regulatory requirements. The system of internal controls within the Company includes written policies and procedures, budgetary controls, supervisory review and monitoring, and various other checks and balances, and safeguards such as password protection to access certain computer systems.

Company Persons are expected to be familiar with, and to adhere strictly to, these internal controls. Responsibility for compliance with these internal controls rests not solely with the Company's accounting personnel, but with all Company Persons involved in approving transactions, supplying documentation for transactions, and recording, processing, summarizing and reporting of transactions and other information required by periodic reports. Any Company Person who believes the Company's books and records are not in accord with these requirements should immediately report the matter.

### **D. Document Management and Retention**

Numerous laws, regulations, and rules require the proper retention of many categories of records and documents that are commonly maintained by companies. In consideration of those legal requirements and the Company's business needs, all Company Persons must maintain records in accordance with these laws.

Any record, in paper or electronic format, relevant to a threatened, anticipated or actual internal or external inquiry, investigation, matter or lawsuit should not be discarded, concealed, falsified, altered, or otherwise made unavailable, once a Company

Person has become aware of the existence of such threatened, anticipated or actual internal or external inquiry, investigation, matter or lawsuit.

All Company Persons must comply with the Company's records management policies. *See, Seven Seas Water Document Retention Policy.* All Company Persons will be notified if such policies and procedures are adopted or if existing policies and procedures are amended.

Any Company Person who believes the Company's document retention is not in accord with these requirements should immediately report the matter.

#### **E. Corporate Advances**

Under law, the Company should not loan money to Company Persons except in limited circumstances. It shall be a violation of the Code for any Company Person to advance Company funds to any other Company Person or to himself or herself except for usual and customary business advances for legitimate corporate purposes, which are approved by a supervisor or pursuant to a corporate credit card for usual and customary, legitimate business purposes. It is the Company's policy that any advance not meeting the foregoing criteria be approved in advance by the Chief Compliance Officer.

Company credit cards are to be used only for authorized, legitimate business purposes. A Company Person will be responsible for any unauthorized charges to a Company credit card. Any Company Person who believes the Company's corporate advances are not in accord with these requirements should immediately report the matter.

#### **V. FAIR DEALING WITH CUSTOMERS, SUPPLIERS, COMPETITORS, AND EMPLOYEES**

The Company does not seek to gain any advantage through the improper use of favors or other inducements, including facilitation payments, involving personal financial gain or advantage to the recipient (generally referred to as bribery). Good judgment and moderation must be exercised to avoid misinterpretation and adverse effect on the reputation of the Company or its personnel or agents. Offering, giving, soliciting or receiving any form of bribe (including facilitation payments) is strictly prohibited whether the other person involved is an employee of a customer or supplier, a public official, or any other person. The Company reserves the right to prohibit the acceptance, retention or giving of a gift, gratuity or business courtesy, meal or entertainment event, regardless of value, as it may determine in its sole discretion. If there are any questions about this policy, or in the case of doubt as to the appropriateness of a gift, employees should contact the Chief Compliance Officer in advance.

##### **A. Giving Gifts**

Business gifts and entertainment are commonly used to build goodwill and strengthen working relationships among business associates. Subject to complying with the Company's policies and applicable law, Company Persons may in certain circumstances provide occasional meals, entertainment, and business gifts in

connection with their work, provided that all such gifts are of nominal value and are not given with the intent or prospect of influencing the recipient's business decision-making. Professional judgment should be exercised based on the prevailing facts and circumstances.

*Cash or cash-equivalent gifts must not be given by a Company Person to any person or organization, even if the cash gift is of token value.* However, subject to complying with applicable law, non-cash gifts, favors and entertainment may be given to non-governmental employees if what is given:

- is consistent with customary business practice;
- cannot be construed as a bribe, pay off or facilitation payment;
- is not in violation of applicable law or ethical standards; and
- will not embarrass the Company or the employee if publicly disclosed.

*See also* subsection below on “Unfair Practices in International Business” for considerations relating to gifts to foreign officials and Section VI “Government Relations” below for considerations relating to gifts to government employees.

## **B. Receiving Gifts**

Gifts, favors, entertainment or other inducements should not be accepted by Company Persons or members of their immediate families from any person or organization that does or seeks to do business with, or is a competitor of, the Company, except as common courtesies usually associated with customary business practices.

*An especially strict standard applies when suppliers are involved. If a gift unduly influences or makes a Company Person feel obligated to “pay back” the other party with business, receipt of the gift is unacceptable. It is not acceptable to accept a gift in cash or cash equivalent in any amount.*

If someone offers a Company Person a gift, favor, entertainment or other inducement that he or she thinks is intended or may be intended as a bribe, he or she is obligated to reject the offer and to report the matter.

## **C. Unfair Competition**

Although the free enterprise system is based upon competition, rules have been imposed stating what can and cannot be done in a competitive environment. The following practices can lead to liability for “unfair competition” and should be avoided. They are violations of this Code.

*Disparagement of Competitors.* While it is not illegal to point out weaknesses in a competitor's service, product or operation; Company Persons should not spread false rumors or misinformation about competitors or make misrepresentations about their businesses. A Company Person should not pass on anecdotal or unverified stories about a competitor's products or services.

*Misrepresentations of Price and Product.* Lies or misrepresentations about the nature, quality or character of the Company's services and products are both illegal and contrary to Company policy. A Company Person should only describe the Company's services and products based on their documented specifications, not based on anecdote or his or her belief that the Company's specifications are too conservative.

#### **D. Antitrust Concerns**

Federal and state antitrust laws are intended to preserve the free enterprise system by ensuring that competition is the primary regulator of the economy. Every corporate decision that involves customers, competitors, and business planning with respect to output, sales and pricing can implicate antitrust concerns. Compliance with the antitrust laws is in the public interest, in the interest of the business community at large, and in our Company's interest.

Failing to recognize antitrust risk is costly. Antitrust litigation can be very expensive and time-consuming. Moreover, violations of the antitrust laws can, among other things, subject you and the Company to the imposition of injunctions, treble damages, and heavy fines. Criminal penalties may also be imposed, and Company Persons may even be imprisoned. For this reason, antitrust compliance should be taken seriously at all levels within the Company.

A primary focus of antitrust laws is on dealings between competitors. In all interactions with actual or potential competitors all employees must follow these rules:

- Do not agree with a competitor or a group of competitors to charge the same prices or to use the same pricing methods, to allocate services, customers, private or governmental payer contracts or territories among yourselves, to boycott or refuse to do business with a provider, vendor, payer or any other third party, or to refrain from the sale or marketing of, or limit the supply of, particular products or services.
- Do not discuss past, present, or future prices, pricing policies, bundling, discounts or allowances, royalties, terms or conditions of sale, costs, choice of customers, territorial markets, production quotas, allocation of customers or territories, or bidding on a job with a competitor.
- Be careful about your conduct. An "agreement" that violates the antitrust laws may be not only a written or oral agreement, but also a "gentlemen's agreement" or a tacit understanding. Such an "agreement" need not be in writing. It can be inferred from conduct, discussions or communications of any sort with a representative of a competitor.
- Make every output-related decision (pricing, volume, etc.) independently, in light of costs and market conditions and competitive prices.

- Carefully monitor trade association activity. These forums frequently create an opportunity for competitors to engage in antitrust violations.

Another focus of antitrust law is how a Company deals with customers, suppliers, contractors and other third parties. Certain practices to discriminate or impose restrictions on customers, suppliers, contractors or other third parties could raise issues, and Company Persons should always consult with the Chief Compliance Officer if there is any concern.

If our Company has a dominant or potentially dominant position with respect to a particular product or market, especially rigorous standards of conduct should be followed. In these circumstances, all Company Persons should:

- Consult with the Chief Compliance Officer before selling at unreasonably low prices or engaging in any bundling practices;
- Keep the Chief Compliance Officer fully informed of competitive strategies and conditions in any areas where the Company may have a significant market position.

Finally, always immediately inform the Chief Compliance Officer if any law enforcement officials request information from the Company or a Company Person concerning the Company or its operations.

## **E. Unfair Practices in International Business**

The Company and Company Persons must comply at all times with all anti-corruption, anti-bribery and anti-kickback laws, rules and regulations in each jurisdiction in which the Company operates. In complying with the potentially overlapping and/or conflicting laws, rules and regulations of various jurisdictions, the Company and Company Persons should always adhere to and seek to follow the most stringent set of laws, rules and regulations to which it or they may be subject.

Under the U.S. Foreign Corrupt Practices Act (“FCPA”), Company Persons are prohibited from making certain gifts to foreign officials. “Foreign officials” include not only persons acting in an official capacity on behalf of a foreign government, agency, department or instrumentality, but also representatives of international organizations, foreign political parties and candidates for foreign public office. The gift is “corrupt” under the FCPA if it is made for the purpose of gaining any “improper advantage” by:

- influencing any act or decision of a foreign official in his official capacity;
- inducing a foreign official to do or omit to do any act in violation of his lawful duty; or
- inducing a foreign official to use his position to affect any decision of the government.

A gift is still “corrupt” even when paid through an intermediary. No Company Person may offer or give any gift to a foreign government official without the advance written approval of the Chief Compliance Officer. Company Persons must be familiar with and abide by the *Seven Seas Water Anti-Corruption and Trade Control Compliance Policy*.

#### **F. Human Trafficking**

Seven Seas Water is committed to supporting the protection and advancement of human rights in our business and throughout our supply chain. With operations around the world, we strive to uphold global standards for responsible business, including equal opportunity, freedom to associate and bargain collectively, and the elimination of child and forced labor. We endeavor to exercise our influence in part by conducting our business operations in ways that attempt to preserve, protect and promote the full range of human rights, such as those described in the United Nations Universal Declaration of Human Rights (UDHR), the International Labour Organization’s Declaration on Fundamental Principles and Rights at Work, and the UN Guiding Principles on Business and Human Rights. *See, Seven Seas Water Supplier Code of Conduct.*

### **VI. GOVERNMENT RELATIONS**

Company Persons must adhere to the highest standards of ethical conduct in all relationships with government employees and must not improperly attempt to influence the actions of any public official.

#### **A. Government Procurement**

The U.S. government and many state and local governments have adopted comprehensive laws and regulations governing their purchases of products and services from private contractors. These laws and regulations are intended to assure that governmental entities receive pricing, terms, and conditions equivalent to those granted to the Company’s most favored commercial customers and that there is full and open competition in contracting. The procurement integrity laws impose restrictions on the relationships between the Company and government procurement officials who have or are engaged personally and substantially in government procurements. Prohibited activities include: (i) offering, discussing, or accepting post-government employment or business opportunities; or (ii) soliciting, obtaining, or disclosing any bid or proposal information, proprietary or source selection information from competitors or government officials. Company Persons working on projects for which the ultimate customer is the U.S. Government must have a working knowledge of and comply with the regulations and laws that govern the acquisition of goods and services by the U.S. government. Company Persons should also ensure that business partners, suppliers, and consultants are aware of and, to the extent practical, in compliance with these legal requirements as well as any similar laws and regulations established in the other non-U.S. jurisdictions in which the Company conducts its business.

When selling products or services to government agencies, the Company is accountable for certifying compliance with applicable procurement laws, regulations, and requirements. Certifications to, and contracts with, government agencies are to be signed

by a Company Person authorized by the relevant Board to sign such documents, based upon knowledge that all requirements have been fully satisfied.

### **B. Payments to Officials**

Under no circumstances should Company Persons make payments or give gifts to officials or employees of the United States Government or any foreign government. Corporate hospitality and the reimbursement of travel expenses involving government officials or employees should be limited to *bona fide* expenses relating to the legitimate promotion of the Company's products and services and in most instances should be approved in advance both by the Chief Compliance Officer and the government organization that employs the person in question.

### **C. Political Contributions**

Company funds, property or services should not be contributed to any political party or committee, or to any candidate for or holder of any office of any government. This policy does not preclude, where lawful, Company expenditures to support or oppose public referendum or separate ballot issues, or, where lawful, the formation and operation of a political action committee, in each case, when reviewed and approved in advance by the Board.

## **VII. COMPLIANCE WITH LAWS, RULES AND REGULATIONS**

### **A. Equal Employment Opportunity**

The Company is committed to a policy of non-discrimination and equal opportunity for all Company Persons and qualified applicants without regard to a person's race, color, religious creed, age, sex, sexual orientation, marital status, national origin, ancestry, present or past history of mental disorder, mental or physical disability, including, but not limited to, blindness and genetic predisposition, or any other factor unrelated to a person's ability to perform the person's job. "Employment decisions" generally mean decisions relating to hiring, recruiting, training, promotions and compensation, but the term may encompass other actions as well.

The Company encourages Company Persons to bring any problem, complaint or concern regarding any alleged employment discrimination to the attention of the Human Resources Department. Company Persons who have concerns regarding conduct they believe is discriminatory should report such matters.

### **B. Sexual Harassment Policy**

The Company is committed to maintaining a collegial work environment in which all individuals are treated with respect and dignity and which is free of sexual harassment. In keeping with this commitment, the Company will not tolerate sexual harassment of Company Persons by anyone, including any supervisor, co-worker, vendor, client or customer, whether in the workplace, at assignments outside the workplace, at Company-sponsored social functions or elsewhere.

Each Company Person has a responsibility to maintain an environment free of sexual harassment. Sexual harassment includes any unwanted or unsolicited conduct or communication on account of an individual's sex which adversely affects that individual's conditions of employment or working environment. Sexual harassment may occur when: (a) submission to the conduct or advances or requests is made either explicitly or implicitly a term or condition of an individual's employment; (b) submission to or rejection of the conduct or advances or requests by an individual is used as the basis for employment decisions affecting such individual; or (c) the conduct or advances or requests have the purpose or effect of substantially interfering with an individual's work performance or creating a hostile, intimidating or offensive working environment.

Other sexually harassing conduct in the work place, such as (a) any abusive or degrading verbal or physical conduct, (b) contact of an offensive and unwelcome nature, or (c) any conduct that interferes with a Company Person's work performance or creates an intimidating, hostile or offensive work environment, by any Company Person is also prohibited.

The following are examples of behavior that may violate this policy:

- Unwelcome and unwanted sexual jokes, language, epithets, advances or propositions;
- Written or oral abuse of a sexual nature, sexually degrading or vulgar words to describe an individual;
- Display of sexually suggestive objects, pictures, posters or cartoons;
- Unwelcome and unwanted comments about an individual's body, sexual prowess or sexual deficiencies;
- Asking questions about sexual conduct;
- Harassment consistently targeted at only one sex, even if the content of the verbal abuse is not sexual;
- Unwelcome touching, leering, whistling, or suggestive, insulting or obscene comments or gestures;
- Demanding sexual favors in exchange for favorable reviews, assignments, promotions, continued employment or promises of the same; and
- Assault or coerced sexual acts.

The Company will not tolerate retaliation of any kind against anyone who complains about sexual harassment in good faith or anyone who participates in good faith in an investigation of a harassment complaint.

Company Persons must also be familiar with and abide by the Company's *Discrimination, Harassment and Retaliation Policy*, set forth in the Employee Handbook, which is given to all Company Persons of the Company and is available from the Human Resources Department or on the Company's internal drive. The Company encourages Company Persons to bring any problem, complaint or concern regarding any alleged sexual harassment to the attention of the Human Resources Department. Company Persons who have concerns regarding conduct they believe constitutes sexual harassment should also report such matters.

### **C. Health, Safety & Environment Laws**

Health, safety and environmental responsibilities are fundamental to the Company's values. Company Persons are responsible for promoting a safe work environment and for ensuring that the Company complies with all provisions of the health, safety, and environmental laws of the United States and of other countries where the Company does business. In addition, Company Persons are required to be familiar with and to abide by the *Workplace Violence and Drug-Free Workplace Policies*, which are available from the Human Resources Department.

The penalties that can be imposed against the Company and Company Persons for failure to comply with health, safety, and environmental laws can be substantial, and include imprisonment and fines.

Company Persons should also be familiar with and abide by the Company's *Safety, Health and Environment Policy*, which is given to all Company Persons and is available from the Human Resources Department, Safety Manager or on the Company's internal drive. A hard copy of the site-specific safety manual is also available at each plant location. The Company encourages Company Persons to bring any problem, complaint or concern regarding any health, safety and environmental concern to the attention of the Safety Manager or Human Resources Department. Company Persons who have concerns regarding health, safety and environmental issues should also make such reports using the Reporting Mechanisms described above.

## **VIII. QUESTIONS UNDER THE CODE AND WAIVERS**

Company Persons are encouraged to consult with the Human Resources Department or the Chief Compliance Officer about any uncertainty or questions they may have under the Code.

If any situation should arise where a course of action would likely result in a violation of the Code but for which the Company Person thinks that a valid reason for the course of action exists, the Company Person should contact the – Chief Compliance Officer to obtain a waiver. Except as noted below, the Chief Compliance Officer will review all the facts surrounding the proposed course of action and will determine whether a waiver from any policy in the Code should be granted.

Waiver requests by an executive officer or a member of any of the Boards shall be referred by the Chief Compliance Officer, with a recommendation, to the relevant Board

or a committee thereof for consideration. If either a majority of the disinterested members on such Board or a committee thereof agrees that the waiver should be granted, it will be granted. If such Board denies the request for a waiver, the waiver will not be granted and the Company Person may not pursue the intended course of action.

It is the Company's policy to grant waivers from the Code only in very limited and compelling circumstances.

## **IX. FREQUENTLY ASKED QUESTIONS**

The following questions and answers address each Company Person's obligation to comply with the Code. The Company has attempted to design procedures that provide confidentiality and, most importantly, freedom from the fear of retaliation for complying with and reporting violations under the Code.

**Q: Do I have a duty to report violations or suspected violations of the Code?**

**A:** Yes, participation in the Code and its compliance program is mandatory. You must immediately report any suspected or actual violation of the Code using the Reporting Mechanisms described above. The Company will keep reports confidential to the fullest extent permitted by applicable law. Failure to report suspected or actual violations is itself a violation of the Code and may subject you to disciplinary action, up to and including termination of employment (or other relationship) or legal action.

**Q: I'm afraid of being fired for raising questions or reporting violations or suspected violations of the Code. Will I be risking my position if I do?**

**A:** The Code contains a clear non-retaliation policy, meaning that if you in good faith report a violation or suspected violation of the Code by the Company, or its agents acting on behalf of the Company, using the Reporting Mechanisms described herein, you will not be at risk of losing your position, nor will you suffer any form of detrimental action as a result of your reporting – even if it is not substantiated in a subsequent investigation. Note, however, that while you will not be disciplined for reporting a violation or suspected violation, you may be subject to discipline with respect to the underlying conduct or violation if you are involved. However, your willingness to cooperate will be taken into consideration. You are entitled to make the report on a confidential and anonymous basis. To the extent an investigation must be initiated, the Company will endeavor to keep confidential any report you make to the extent permitted by applicable law.

You are encouraged to pursue all internal reporting channels through completion and reasonably await and consider the results of all internal investigations before reporting matters outside of the Company. We have instituted the procedures described in this Code, including procedures to make anonymous submissions, to facilitate internal investigations.

You should also consider leaving, but are not required to leave, your name or a contact number when submitting a report. Such information may facilitate a more

thorough and efficient investigation. The Chief Compliance Officer will strive to maintain the integrity and confidentiality of all compliance-related communications. However, in certain circumstances, the identity of the person reporting the issue may become known or may need to be revealed, particularly if federal or state enforcement authorities become involved in the investigation. The Company cannot guarantee confidentiality when material evidence of a violation of the law is disclosed or if the person is identified during the normal course of an investigation.

**Q: How are suspected violations investigated under the Code?**

**A:** When a suspected violation is reported using the Reporting Mechanisms described herein, the Human Resource Department or Chief Compliance Officer (or his designee) will gather information about the allegation by interviewing the Company Person reporting the suspected violation, any Company Person who is accused of the violation and/or any other persons to determine if a factual basis for the allegation exists. However, depending on the nature of the suspected violation and the source of the report, the respective Board, at its discretion, may choose to investigate the suspected violation directly. The reporting Company Person's immediate supervisor will not be involved in the investigation if the reported violation involved that supervisor.

If the report is not substantiated, the reporting Company Person will be informed and at that time will be asked for any additional information not previously communicated. If there is no additional information, the Chief Compliance Officer may close the matter as unsubstantiated.

If the allegation is substantiated, the Chief Compliance Officer will make a judgment as to the appropriate disciplinary response. In some instances, the Chief Compliance Officer will make a recommendation to the relevant Board of the Company for its approval. Such Board's decision as to disciplinary and corrective action will be final. In other instances, the Chief Compliance Officer may refer the violation to the individual's supervisor or the Human Resources Department for appropriate disciplinary action, as the facts may dictate.

The Chief Compliance Officer will provide a summary of all significant matters considered under the Code to each Board or a committee thereof at each regular meeting thereof or sooner if warranted by the severity of the matter.

**Q: Do I have to participate in any investigation under the Code?**

**A:** Your full good faith cooperation with any pending investigation under the Code is a condition of your continued relationship with the Company. The refusal to cooperate fully and in good faith with any investigation is a violation of the Code and grounds for discipline, up to and including termination.

**Q: What are the consequences of violating the Code?**

**A:** As explained above, Company Persons who violate the Code may be subject to discipline, up to and including termination of employment (or other

relationship) and legal action. Company Persons who violate the Code may also violate federal, state, local or foreign laws, regulations or policies. Such Company Persons may be subject to prosecution, imprisonment and fines, and may be required to make reimbursement to the Company, the government or any other person for losses resulting from the violation. They may be subject to punitive or treble damages depending on the severity of the violation and applicable law.

**Q: What if I have questions under the Code or want to obtain a waiver under any provision of the Code?**

**A:** The Human Resource Department or the Chief Compliance Officer can help answer questions you may have about this Code. You should not pursue a course of action that is unclear under the Code without first consulting the Human Resource Department or the Chief Compliance Officer, and if appropriate, obtaining a waiver.

**APPENDIX A**

**FORM EMPLOYEE ACKNOWLEDGEMENT AND AGREEMENT TO COMPLY WITH CODE**

I have read the *Seven Seas Water Code of Business Conduct and Ethics* and Appendices B and C thereto (the "Code"). I have obtained an explanation from the Company of any provision about which I may have had a question. I agree to abide by the provisions of the Code. Based on my review, I acknowledge that:

\_\_\_\_\_ To the best of my knowledge, I am not in violation of, or aware of any violation by others of, any provision contained in the Code;

OR

\_\_\_\_\_ I have made a full disclosure below of the facts regarding any possible violation of the provisions set forth in the Code.

In addition, I understand that I am required to report any suspected or actual violation of the Code, and that I may make such reports on a fully anonymous basis through the mechanisms described in this Code. I understand that I am required to cooperate fully with the Company in connection with the investigation of any suspected violation. I understand that my failure to comply with the Code or its procedures may result in disciplinary action, up to and including termination.

By: \_\_\_\_\_ Date: \_\_\_\_\_  
Name

(Please print): \_\_\_\_\_

Department/Location: \_\_\_\_\_

**APPENDIX B**

**SEVEN SEAS WATER**

**WHISTLEBLOWER POLICY**

## SEVEN SEAS WATER WHISTLEBLOWER POLICY

### I. PURPOSE OF THIS WHISTLEBLOWER POLICY

The purpose of this Whistleblower Policy (the “Policy”) is to:(i) encourage employees of Seven Seas Water<sup>4</sup>(also referred to as the “Company”), as well as all stakeholder groups (including investors and shareholders, regulators and government representatives, and special interest groups), consultants, advisors and anyone who provides services to, on behalf of, the Company, to report any violation or suspected violation of the Company's Code of Business Conduct and Ethics (the “Code” and available on the Company's internal drive), including, but not limited to, suspected violations of applicable laws, rules and regulations, accounting issues, and any law relating to fraud against stakeholders; (ii) provide the employees and stakeholders with a confidential means for reporting the violations or suspected violations; (iii) protect individuals who report violations or suspected violations in good faith;and (iv) effectively communicate the Policy.

Each employee has a responsibility, and is required, to report a violation or suspected violation of the Code, or other concerns identified below, using the proper channels (defined below as “Reporting Mechanisms”). Additionally, the Company also encourages employees and stakeholders to report using the Reporting Mechanisms for any concern an employee may have with respect to the Company, including, but not limited to, concerns with the Company's business or operations or any other issue concerning the Company and their employment with the Company.

The types of concerns that should be reported (hereafter referred to as “Reportable Concerns”) include, but are not limited to, the following:

Ethical Violations	Violation of Securities Laws
Unsafe Working Conditions	Wrongful Discharge
Sexual Harassment	Internal Controls
Theft	Vandalism and Sabotage
Discrimination	Improper Conduct
Alcohol and Substance Abuse	Conduct Violations
Fraud	Threats and Bullying
Questionable Accounting or Auditing Matters	Bribery and Kickbacks
Conflict of Interest	Misuse of Company Property
Theft and Embezzlement	Violation of Company Policy
Violation of applicable laws, rules and regulations	Falsification of Contract, Reports or Records
	Trade Controls Violations

---

<sup>4</sup> “Seven Seas Water” means Seven Seas Water Corporation, AUC Group, LLC, Bluefin Water Solutions LLC, Marlin Water Solutions Co, Yellowfin Water Solutions Co., and Tarpon Water Solutions Ltd, as well as their respective affiliates and subsidiaries

The Company prohibits any type of corporate fraud and is committed to protecting employees from adverse consequences in connection with any whistleblowing activities. Reports made to the Whistleblower Hotline (as defined below) will be provided for investigation directly to the Chief Compliance Officer, Human Resources Director, and a member of the Boards on an anonymous and confidential basis.

## II. SCOPE OF THE WHISTLEBLOWER POLICY

Every Company employee must comply with this Policy. This Policy will be made available to active employees and to every new employee as part of his or her initial orientation. Each employee must be familiar with this Policy and agree to abide by it.

## III. PROTECTION OF WHISTLEBLOWERS

Employees should immediately report to the Company any suspected violations of the Code, including, but not limited to, the Reportable Concerns noted above. Any employee who makes a report of a matter, genuinely and in good faith, which s/he reasonably believes constitutes a Code violation, including, but not limited to, the Reportable Concerns noted above, will not be at risk of losing their job, nor will they suffer any form of detrimental action as a result of their reporting - even if it is not substantiated in a subsequent investigation. However, any false, bad faith, or malicious reporting or allegations may lead to appropriate disciplinary and legal action, up to and including termination of employment.

## IV. HOW TO MAKE A REPORT

If any violation, or suspected violation, of the Code is known to an employee, that employee is responsible, and required, to report violations using one or both of the following methods (referred to herein as the “Reporting Mechanisms”):

- (1) **Reporting through the Supervisory Chain.** Violations can be reported through either the employee's immediate supervisor or with a more seniorsupervisor.
- (2) **Contacting the Chief Compliance Officer.** Violations can be reported to the Chief Compliance Officer or the Human Resources Department.
- (3) **Contacting a member of the Board.** Please reach out to the Chief Compliance Officer or the Company’s Human Resources department for current information.
- (4) **Reporting through the Whistleblowing Hotline.** Our Whistleblowing Hotline is an independent third-party service that provides an anonymous and confidential reporting mechanism for any violations, or suspected violations. The Whistleblowing Hotline can be accessed 24 hours a day, seven days a week. Individuals who call the Hotline need not identify themselves. The Whistleblowing Hotline telephone number for US employees is: 1-844-279-8283. The Whistleblowing Hotline telephone number for non-US employees can be found on the Company’s dedicated internet address. The internet link is: <https://secure.ethicspoint.com/domain/media/en/gui/41684/index.html>

## V. CHANGES TO THE POLICY AND AVAILABILITY TOEMPLOYEES

This Policy shall be reviewed and updated as appropriate. Amendments to this policy may be necessary from time to time due to changes in the law or the Company's operations. This Policy has been approved by the Board of Directors of each Company and any material changes to this Policy must be approved by the relevant Board of Directors. All employees

will receive notice when this Policy is changed. The current version of this Policy will be available on the Company's internal drive or is available by contacting the Human Resources department. The Policy shall be presented to the Company Employees at least once per year.

**APPENDIX C**

**SEVEN SEAS WATER ANTI-CORRUPTION AND TRADE CONTROLS  
COMPLIANCE POLICY**

## **SEVEN SEAS WATER ANTI-CORRUPTION AND TRADE CONTROLS COMPLIANCE POLICY**

Seven Seas Water<sup>5</sup> (referred to herein as “Company,” “we,” or the “SSW Group”) 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. This Anti-Corruption and Trade Compliance Policy (the “Policy”) applies to all personnel and agents of the SSW Group, including all officers and other employees of the SSW Group, and all persons engaged to perform work for the SSW Group, including temporary agency personnel, non-employee agents acting on the SSW Group’s behalf, and contractor personnel (collectively, “Company Persons”). Any questions concerning this Policy should be immediately referred to the “Chief Compliance Officer” (or “CCO”), or anyone working under the authority of the CCO (“Compliance Officer”). The Company’s senior management is committed to fostering a culture of compliance with this Policy and the related Anti-Corruption and Trade Control Compliance Procedures, and to supporting and delegating sufficient authority and autonomy to the CCO.

The Company is committed to complying with all applicable United States laws, including the U.S. Foreign Corrupt Practices Act of 1977 (the “FCPA”), and any other applicable anti-bribery and anti-corruption laws in the countries in which the SSW Group does business (together, “Anti-Corruption Laws”). These obligations to comply with Anti-Corruption Laws extend to all Company Persons as defined in the Company’s Code of Business Conduct and Ethics.

This Policy contains information intended to reduce the risk of corruption and bribery from occurring in the Company’s activities and to familiarize you with the specific requirements and prohibitions applicable to our operations under Anti-Corruption Laws, including but not limited to, the FCPA, the UK Bribery Act, and similar Anti-Corruption Laws. You also have a broader obligation to comply with all Local Laws in addition to the Anti-Corruption Laws specifically discussed in this Policy. Nothing in this Policy limits the scope or requirements of the Company’s Code of Business Conduct and Ethics or other compliance policies. This Policy provides guidance to ensure that Company personnel, and the Company’s agents and business partners, do not knowingly or unknowingly compromise Company values or violate any Anti-Corruption Laws.

As a Company Person, you have an obligation to review and understand this Policy, attend any FCPA or anti-corruption training that the Company may require you to attend, seek guidance on anti-corruption issues as they arise, and report suspected FCPA or similar violations promptly.

It is the policy of Seven Seas Water to comply with all sanctions and export control laws and regulations of the US, EU, UK, UN, and all applicable sanctions and export control laws and regulations in the countries in which the SSW Group does business (together, “Trade Control Laws”). This Policy addresses what we must do in order to comply with these Trade Control Laws. All employees and other persons or entities working on behalf of the SSW Group share the responsibility and accountability for complying with relevant Trade Control Laws and this Policy.

All parties subject to this Policy must be certain, prior to any transaction, that any necessary

---

<sup>5</sup> “Seven Seas Water” means Seven Seas Water Corporation, AUC Group, LLC, Bluefin Water Solutions LLC, Marlin Water Solutions Co, Yellowfin Water Solutions Co., and Tarpon Water Solutions Ltd, as well as their respective affiliates and subsidiaries.

export notifications have been made and appropriate export licenses have been obtained, and that the transaction is lawful under US, EU, UK, and UN laws, as well as other Trade Control Laws, where applicable.

Failure to comply with Anti-Corruption Laws or Trade Control Laws may result in civil and/or criminal penalties, as well as significant harm to the SSW Group's reputation. Such a failure may also result in civil and criminal penalties being imposed against the Company Persons involved. Failure to comply with this Policy may also result in disciplinary action being taken by the SSW Group.

Thank you for your support in ensuring that the SSW Group's compliance with all applicable Anti-Corruption and Trade Control Laws is a success.

Sincerely,

Michael Noone  
General Counsel, Chief Compliance Officer, SSW Group

## I. ANTI-CORRUPTION POLICY

### A. THE FCPA

#### 1. Overview

The FCPA contains two components, which are informally known as its “anti-bribery provisions” and its “accounting provisions.” In summary, the “anti-bribery provisions” prohibit the SSW Group and its Company Persons around the world from offering, authorizing, promising, directing or providing anything of value to any non-U.S. government official for the purpose of influencing that person to assist the SSW Group in obtaining or retaining business or securing an improper business advantage. Individuals and companies may also be penalized if they order, authorize, or assist someone else to violate the anti-bribery provisions, or if they conspire to violate those provisions.

In addition to prohibiting improper payments, the FCPA also contains “accounting provisions” that impose additional record-keeping and internal control requirements on public companies. Although the SSW Group is not a public issuer, the SSW Group is nonetheless committed to maintaining strong internal controls and ensuring that its books and records are accurate. Any mischaracterization or omission of any transaction on the SSW Group’s books, or any failure to maintain proper accounting controls, is prohibited.

#### 2. FCPA Penalties

Under the anti-bribery provisions of the FCPA, any SSW Group director, officer, employee, representative, agent, business partner, or person acting on behalf of the SSW Group who willfully violates the FCPA may be liable for up to \$10,000 in civil fines and up to \$100,000 in criminal fines and may be imprisoned for up to five years. The SSW Group may be liable for civil fines up to \$10,000 and criminal fines up to \$2 million. Further, under a U.S. federal statute known as the Alternative Fines Act, courts may impose significantly higher fines on defendants than those provided by the FCPA up to twice the benefit a defendant sought to obtain by offering or making a corrupt payment. Fines imposed on individuals may not be paid by their employer.

In addition, an FCPA violation could result in other adverse consequences such as suspension or debarment from government contracts, revocation or suspension of export license privileges, shareholder lawsuits, disgorgement, and long-term damage to the SSW Group or an individual’s reputation.

#### 3. FCPA Provisions and What They Mean

Included below are summaries and explanations of some important FCPA provisions to assist you in your general understanding of the FCPA’s requirements. You can find the full text of the FCPA at the Department of Justice’s website, <http://www.justice.gov/criminal/fraud/fcpa/>, which also contains translations of the FCPA in many languages.

- **The FCPA broadly defines “foreign officials.”** A foreign official (“Government Official”) is someone who acts as an elected official of a non-U.S. government, acts as an officer or employee of any government department, acts as an employee, officer, or director of a state-owned or quasi-governmental enterprise, or acts in an official capacity for or on behalf of a foreign government even if that person is not employed by the government (*e.g.*, a government consultant). Employees of state-owned enterprises or government-controlled entities, as well as officials from public international

organizations, also qualify as foreign officials. In certain instances, the FCPA may also apply to relatives of Government Officials.

- Examples of Government Officials under the FCPA may include employees of government-owned hospitals, utility companies, and universities.
- **The FCPA prohibits making, authorizing, or promising improper payments.** You do not need to make a payment for liability to attach under the FCPA. The mere offer or promise of a payment can lead to a violation of the statute.
- **The FCPA prohibits payment of money or anything of value.** The FCPA extends to payments of anything of value – not just payments of cash. There is no minimum threshold or materiality requirement for corrupt payments.
  - Prohibited payments can take many forms, including the purchase of a Government Official’s property or services at inflated prices, entertainment, charitable donations, travel expenses, loans with favorable terms, scholarships, cars or sports equipment, or anything else of value.

**The following are examples of bribes or improper payments under the FCPA:**

- Promising or making payments or giving something of value to a Government Official in order to receive or renew a license or permit or to obtain an approval that the SSW Group needs to continue its business;
- Promising or making payments or giving something of value to a Government Official that is intended to influence implementation of a law that is beneficial to the SSW Group’s business or to influence the repeal of a law that is adverse to the SSW Group’s business;
- Promising or making payments or giving something of value to a Government Official in exchange for overlooking or forgiving a regulatory compliance mistake or violation;
- Promising or making payments or giving something of value to a Government Official or political parties in connection with transactions or proposed transactions related to the SSW Group’s products or services; or
- Promising or making payments to a Government Official intended to influence acts and decisions that would help the SSW Group to win a deal or prevent the SSW Group from losing a deal.
- **The FCPA prohibits both direct and indirect payments.** In addition to direct payments to foreign Government Officials, indirect payments through an agent, partner, subsidiary, consultant, or any other third-party may also give rise to liability. The FCPA prohibits payments to any person while “knowing” that any part of the proceeds will be provided to or otherwise used to influence the acts of a non-U.S. official.
- **The FCPA does not require quid pro quo agreement.** The SEC and U.S. courts have made clear that an arrangement need not be of a “quid pro quo” nature to be corrupt. Any attempt to favorably influence foreign officials, even if that simply includes purchasing their good will, may be considered securing an improper advantage and a violation of the FCPA.

- **Exceptions to the FCPA for “facilitating payments” are extremely narrow. You may not make facilitating payments when working on behalf of the SSW Group.** Under very narrow and limited circumstances, the FCPA permits payments to Government Officials where the purpose of the payment is to expedite a “routine government action.” Routine government action refers only to those actions that are “ordinarily and commonly performed” by government officials. These payments cannot be made to influence any discretionary decision by an official and must be allowed under local laws.
  - Facilitation payments must be fixed, non-discretionary, and available to all businesses.
  - This exception does not apply to decisions by foreign officials to award or maintain business.
  - Facilitating payments, even if they do not violate the FCPA, may violate the laws of other countries. For example, facilitation payments are illegal under the UK Bribery Act.
  
- **Exceptions for “Reasonable and Bona Fide Expenses.”** The FCPA permits payments to foreign officials for reasonable and bona fide expenses directly related to a promotion, demonstration, or explanation of a company’s products and services. However, you must be extremely careful when making such payments and keep the following rules in mind:
  - Do not extend any invitation for travel to any Government Official, government employee, or political party official or candidate for political office, without the prior approval of the Compliance Officer.
  - Any travel or entertainment expenses must be limited solely to those individuals necessary for the furtherance of the SSW Group’s business. You cannot pay or promise to pay any travel or entertainment expenses for spouses or guests of your invitees.
  - All travel and entertainment expenses must be accurately and adequately documented in the books and records of the SSW Group; you must not misstate the purpose or value of these expenses.
  - Legitimate gifts, meals and entertainment are permitted only if they are of nominal value, infrequent, and not offered for an improper purpose.
  - It is your obligation to ensure that a payment qualifies as a “reasonable and bona fide expense.” You must review and comply with the Giving Gifts, Receiving Gifts, and Payments to Officials sections of the Code of Business Conduct and Ethics before you offer gifts, hospitality, or travel. If you have any questions or uncertainty, you must consult the Compliance Officer.
  - As noted in the Code of Business Conduct and Ethics, **cash or cash-equivalent gifts must not be given to any person or organization, even if the cash gift is of a token value. It is likewise not acceptable for an SSW Group Person to accept a gift in cash or cash equivalent in any amount.**

- **Record-keeping and internal controls requirements.** The FCPA requires public companies to maintain detailed and accurate accounting records and internal controls. Although the SSW Group is not a public issuer, the SSW Group is committed to the highest levels of ethical business conduct, and the SSW Group requires that all Company Persons comply with the record-keeping and accounting provisions of the FCPA. Accordingly:
  - You must not create any false, incomplete, or misleading entries or records.
  - You must not maintain any undisclosed or unrecorded corporate funds for miscellaneous expenses.
- **Willful ignorance and similar bad acts by others are not valid defenses.** Willfully ignoring FCPA warning signs in an attempt to avoid gaining actual knowledge of a violation is not a valid defense. Similarly, arguments that bribes or improper payments are part of the business culture in a particular country or industry, or are part of the costs of doing business in a particular country, are not valid defenses.
- **Red Flags.** Be mindful of “red flags” that may require further inquiry to ensure that improper payments are not being directed to Government Officials. See Chapter 1 of the Anti-Corruption and Trade Control Procedures for further information.

## **B. UK Bribery Act**

### **1. Overview**

Similar to the FCPA, the UK Bribery Act of 2010 (“UK Bribery Act”) is also designed to limit bribery and corruption by commercial organizations. The UK Bribery Act extends its jurisdiction to all businesses that conduct some part of their business in the UK, even if the bribe or improper conduct at issue happens outside the UK. In particular, the UK Bribery Act impacts the SSW Group’s operations in the British Virgin Islands or the Turks and Caicos Islands, both of which are British Overseas Territories.

In a number of ways, the UK Bribery Act is even broader than the FCPA. For example, the UK Bribery Act prohibits bribes to any individuals, not just Government Officials. In addition, the UK Bribery Act prohibits the receipt or offer of a bribe. The SSW Group requires full compliance with the UK Bribery Act and any other applicable Anti-Corruption Laws.

### **2. Additional Factors to Consider to Ensure Compliance with the UK Bribery Act**

Adherence to the principles outlined above regarding the FCPA will also assist the SSW Group, Company Persons, and the SSW Group’s business partners around the world from violating the UK Bribery Act and other similar anti-corruption laws. Included below are a few additional factors to consider to ensure compliance with the UK Bribery Act. You can find the full text of the UK Bribery Act at <https://www.justice.gov.uk/legislation/bribery>, which also contains guidance by the UK government regarding the law. You are encouraged to review these materials and/or contact the Corporate Compliance Officer if you have any questions or require any additional information.

- **The UK Bribery Act prohibits payments to any persons, not just to Government Officials.** One of the biggest differences between the FCPA and the UK Bribery Act is

that, while the FCPA only applies to the corruption of non-U.S. officials, the Bribery Act prohibits corrupt payments to any person, not just a foreign government official. Thus, the UK Bribery Act prohibits commercial bribery and private-to-private bribery. (However, please note that although the FCPA may be limited to foreign officials, there are other U.S. laws that cover commercial bribery and improper business conduct. The SSW Group expects its personnel and its business partners to fully adhere to all laws and always act with the highest level of business ethics.)

To commit the offense of bribing another person under the UK Bribery Act, the bribery must intend to bring about or to reward improper performance of any function or activity. This function or activity may be within the private or public sector, and the test of whether it has been improperly performed is an objective test of what a reasonable person in the UK would expect in relation to the performance of the type of function or activity concerned.

- **The UK Bribery Act prohibits giving or receiving bribes.** Another way in which the UK Bribery Act is broader than the FCPA is that it makes it an offense to request, to agree to receive, or to accept a bribe. The FCPA, on the other hand, applies only to persons giving or offering an improper payment. (However, even though the FCPA does not prohibit receiving or requesting bribes, the SSW Group prohibits any of its personnel or business partners from engaging in such unethical conduct.)
- **The UK Bribery Act does not require any corrupt intent for payments to foreign officials.** The UK Bribery Act contains a stand-alone offense of bribing a public official (in addition to the general bribery offense that applies to all recipients and does not require a payment to a public official). Unlike a violation of the anti-bribery provisions of the FCPA, which require the government to prove a corrupt intent, the UK Bribery Act offense of bribing a public official does not require the government to prove a corrupt intent, thus making it even easier to establish a violation.
- **The UK Bribery Act creates a strict liability offense for organizations that fail to prevent bribery.** The UK Bribery Act creates a strict liability corporate offense for a company's failure to prevent bribery unless the SSW Group can establish that it had "adequate procedures" in place to prevent bribery. Given that the UK Bribery Act extends to acts of "associated persons," anyone who performs services for or on behalf of a commercial organization can cause it to suffer great harm. Accordingly, the SSW Group requires its personnel to be especially vigilant in ensuring that neither they nor their agents and business partners violate the UK Bribery Act.
- **The UK Bribery Act imposes significant penalties on both the individual and the SSW Group.** An individual found to have committed an offense under the UK Bribery Act is subject to imprisonment of up to ten years and/or an unlimited fine. A company found to have committed an offense is subject to an unlimited fine.

### C. DILIGENCE ON BUSINESS PARTNERS

In some instances, it may be necessary to use a third-party agent, consultant, distributor, or joint venture partner to help conduct the SSW Group's business. In such instances, all SSW Group personnel have an obligation to ensure that any third-party agents or business partners with whom they seek to establish a relationship on behalf of the SSW Group are properly investigated to

ensure compliance with the FCPA, UK Bribery Act, and this Policy.

One step to ensure compliance is to conduct due diligence on every agent or partner who conducts business in any foreign jurisdiction before entering into any third-party relationship, contract, or agreement in accordance with the SSW Group's Anti-Corruption and Trade Controls Compliance Procedures. Before entering into such relationships, SSW Group personnel should undertake the following due diligence:

- Checking public sources of information, including internet searches and published press reports concerning the agent;
- Checking with business references provided by the potential third-party contractors;
- Interviewing the third-party agent; and
- Seeking information about the third-party agent's compliance policies and seeking their affirmation that they will comply with all applicable law when conducting business on behalf of the SSW Group.

The Compliance Officer can provide you with materials regarding proper due diligence and can direct you to individuals who can assist in performing such due diligence. If you have concerns about the type and scope of diligence required by a particular situation, it is your duty and responsibility to raise any questions or concerns with the Compliance Officer. Any third-party working on behalf of the SSW Group, including but not limited to consultants, must receive approval from the Compliance Officer prior to entering into an agreement with any Government Official.

Additional investigation may be necessary in particular circumstances, (*e.g.*, when the third-party will be interacting with a government agency or foreign official; in a high-risk jurisdiction) or depending on the results of the above suggested steps. SSW Group personnel should consult with the Compliance Officer when conducting due diligence on third-parties and partner businesses.

All due diligence into third-party agents and business partners should be documented. In order to fulfill the "due diligence" principle, the SSW Group reserves the right not to enter into agreements with counterparties that were deemed unreliable by the results of the audit/corruption check.

The SSW Group shall extend the basic principles and prohibitions of this Policy to agents and third-parties by means of an anti-corruption clause to be included in the contracts/agreements concluded by the SSW Group with the said persons. The development of an anti-corruption clause shall be carried out by the legal department of the SSW Group with the involvement of the Compliance Officer, taking into account the requirements of Local Laws and this Policy. An anti-corruption clause is subject to inclusion in all concluded contracts of the SSW Group.

#### **D. SEEKING GUIDANCE ON ANTI-CORRUPTION ISSUES**

The SSW Group's Chief Compliance Officer and his/her delegated representative(s) are responsible for implementing and providing guidance and interpretation on matters related to this Policy.

**SSW Group personnel with questions about the FCPA, UK Bribery Act or other Anti-Corruption Laws, or who are uncertain of the requirements of the Policy, are obligated to seek guidance from the Compliance Officer.**

The Compliance Officer also has responsibility for investigating, or overseeing the investigation of, any information or allegations concerning possible violations of anti-corruption laws or other unethical or improper business conduct. The Compliance Officer will have authority to retain and consult with outside legal counsel to assist in carrying out his duties.

It is understood that SSW Group personnel will often go to their immediate supervisor to seek guidance on ethics-related issues or report potential violations of the Code of Business Conduct and Ethics, this Policy or other rules and regulations. However, there may be situations in which SSW Group Persons do not wish to raise such issues with their supervisors. Such situations include instances where the conduct in question involves a supervisor, where the employee has reported the conduct previously and does not believe that the supervisor has dealt with it properly or where the employee does not feel that the matter can be appropriately discussed with his or her supervisor. In these types of situations, SSW Group Persons should raise the matter with the Compliance Officer, either directly or anonymously.

Note: Each SSW Group officer, director, or employee has an independent and continuing obligation to ensure compliance with the FCPA, UK Bribery Act and any other applicable laws. Simply reporting potential issues to a supervisor does not absolve you from responsibility relating to improper conduct.

## **II. Trade Control Compliance Policy**

The SSW Group's Trade Control Compliance Policy is designed to promote compliance with the economic sanctions and export controls maintained by the United States, European Union, United Kingdom, United Nations, and with similar sanctions and export control laws and regulations of other nations applicable to the Company's business. This Policy and the related Trade Control Procedures reflect the US Office of Foreign Assets Control's Framework for Compliance Commitments and the US Bureau of Industry and Security's Export Compliance Guidelines, which both provide guidance and essential components for developing an effective, risk-based sanctions and export control compliance program. This Policy and the related Procedures also account for the SSW Group's identified risks based on its customers, counterparties, services, and geography.

### **A. OVERVIEW OF US ECONOMIC SANCTIONS AND EXPORT CONTROLS**

US sanctions and export control laws are designed to protect US national security and support US foreign policy.

#### **1. US ECONOMIC SANCTIONS**

US economic sanctions are primarily administered by the US Department of the Treasury's Office of Foreign Assets Control ("OFAC"). They prohibit commercial and other transactions, by US persons or involving the United States, with certain countries/regions or specific persons (individuals and entities) targeted under a variety of sanctions regimes. Although US sanctions prohibitions primarily apply to US persons, such prohibitions may also apply to persons engaged in transactions involving the United States, such as US dollar-denominated funds transfers that transit a bank in the United States.

Even unintentional conduct can give rise to a US sanctions violation. Sanctions measures range from broad prohibitions on most dealings with the targeted countries/regions ("comprehensive sanctions") to restrictions on certain dealings with certain persons ("list-based sanctions"). The United States currently maintains comprehensive economic sanctions programs against Iran, Syria, Crimea, North Korea, and Cuba. List-based sanctions provide that US persons

may not engage in specified transactions with persons designated by the United States for engaging in certain activities contrary to US foreign policy or national security interests (“Restricted Parties”). The United States maintains and periodically updates various lists of individuals and entities subject to various such restrictions (for example, the List of Specially Designated Nationals and Blocked Persons (“SDN List”)<sup>6</sup> and the Sectoral Sanctions Identifications List,<sup>7</sup> among others).

In addition, the US can impose sanctions on non-US persons engaged in sanctionable activities, even without a connection to the United States. These sanctions measures are sometimes referred to as “secondary” sanctions and can include, for example, exclusion from the US financial system and commercial markets (e.g., prohibiting exports from the United States, designation as an SDN, or prohibiting foreign exchange involving US banks). Sanctionable activities that can lead to the imposition of such sanctions measures can include, among other things, dealings with Restricted Parties, such as parties listed on the SDN or SSI Lists, or activities relating to weapons proliferation, narcotics trafficking, or terrorism.

With regard to US sanctions on Venezuela, the United States currently maintains sanctions blocking the property of the Government of Venezuela (which is broadly defined to include, among others, entities owned or controlled by or acting for or on behalf of the Government of Venezuela) and certain Venezuelan entities and individuals identified on the SDN List, including among others the Central Bank of Venezuela and *Petróleos de Venezuela, S.A.* (“PdVSA”), the Venezuelan state-owned oil company (and entities owned 50% or more by such persons). The United States imposes additional restrictions on certain loans to, extensions of credit to, dealings in debt of, and financings or dealings in equity of both the Government of Venezuela and PdVSA.

## 2. US EXPORT CONTROLS

The US Department of Commerce Bureau of Industry and Security (“BIS”) is responsible for regulating the export of “dual-use” items (*i.e.*, items with both military and commercial applications). Many commercial items that are subject to regulation under the US Export Administration Regulations (“EAR”) might not have obvious military uses or purposes. These regulations restrict the transmission, shipment, or transfer of certain goods, software, technology or certain kinds of data (collectively “items” that are “subject to the EAR”) to a foreign national, whether inside or outside the United States. The United States also maintains and periodically updates various lists of parties subject to export control restrictions (such as the Entity List,<sup>8</sup> among others).

The term “export” has an extremely broad definition for purposes of US export controls. Due to the broad definition, the scope of these laws is not always self-evident. For example, any

---

<sup>6</sup> The “SDN List” is OFAC’s list of persons primarily subject to an asset blocking under US economic sanctions. US persons and others subject to US jurisdiction are prohibited from engaging in any dealings with any person (individual or entity) on the OFAC SDN List, or any entity owned 50 percent or more by one or more such entities, absent an applicable authorization or exemption. US persons must block all property and interests in property of an SDN that come within their possession or control, and report such blocking to OFAC within ten days. <https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists>.

<sup>7</sup> The “SSI List” is a list of Russian persons subject to limited restrictions on dealings in certain “new debt” and, as applicable, “new equity” involving US persons or within the United States. Additional restrictions may also apply to certain activities relating to Arctic, deep water, or shale oil projects or involving certain SSI entities. <https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list/sectoral-sanctions-identifications-ssi-list>.

<sup>8</sup> The “Entity List” is a list of entities whose participation in a transaction can trigger enhanced EAR license requirements for any item subject to US export jurisdiction (imposed in addition to any license requirements triggered by any other EAR provisions). The list specifies the license requirements that apply to each listed entity. <https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list>.

instructions or technical information regarding the production of a substrate that is transferred in the United States from a US employee to a foreign employee involves an “export” for purposes of US export controls. Items that can be exported include commodities, software, technology, and technical information.

### **3. IMPORTANCE OF COMPLIANCE – COST OF VIOLATIONS**

Violations of US Trade Control Laws carry substantial penalties, both civil and criminal. Civil penalties for trade control violations currently can reach approximately \$300,000, or twice the value of the relevant transaction, for each violation, and criminal penalties include a fine of up to \$1 million per violation. Individuals can also face criminal penalties of up to 20 years in prison. Because of the broad scope of the laws, a single commercial transaction could involve several violations. In addition, individuals and companies may be required to forfeit the goods or proceeds from a transaction in violation of these laws. The government may further penalize violators by taking away export privileges, such as by prohibiting other parties from doing business with companies and individuals who have violated the law.

## **B. OVERVIEW OF EU AND UK TRADE CONTROLS**

The European Union (“EU”) is currently composed of 27 Member States (“EU Member States”); the United Kingdom (“UK”) is no longer a Member State but continues to apply EU laws until the end of a transition period bound to expire on 31 December 2020. (After the transition period ends, unless extended, EU sanctions will no longer apply in the UK and autonomous UK sanctions regimes will enter into force under the Sanctions and Anti-Money Laundering Act 2018.) The EU’s economic sanctions and trade controls serve to advance EU foreign policy, contribute to international peace and security, and influence change in foreign countries, entities or individuals. While the EU tends to act as one body for the purposes of economic sanctions or export controls, individual EU Member States and the UK may sometimes impose greater restrictions. In addition, military export controls largely remain within the remit of the individual EU Member States and the UK.

### **1. Jurisdiction of EU and UK Laws and Regulations**

The EU’s economic sanctions regime applies to any activities where there is EU jurisdiction, i.e. where there is an “EU nexus.” As a general rule, there is EU sanctions jurisdiction over any activity within the EU territory, its airspace, or on board any aircraft or vessel under an EU Member State’s jurisdiction. Persons and legal persons, entities and bodies that are nationals of, or incorporated or constituted under the laws of, an EU Member State are also subject to EU sanctions jurisdiction, regardless of whether they are located inside or outside EU territory. Accordingly, there may be EU sanctions jurisdiction over certain “brokering” activities, i.e. when EU persons or companies negotiate or arrange transfer of covered items between third countries. Finally, any legal person, entity or body that does business, in whole or in part, within the EU is subject to EU sanctions jurisdiction.

As regards overseas territories of the UK or EU Member States (such as the British Virgin Islands, Turks and Caicos Islands, Curacao, and St Maarten), even if such overseas territories are not as such EU Member States, the EU sanctions may apply. This will be the case if the respective overseas territory has implemented the substance of EU sanctions under local rules or must follow EU sanctions under the legal regime that applies to it. It will therefore be important to check the EU sanctions status as it varies depending on the particular overseas territory.

### **2. Economic Sanctions**

The EU broadly has two different sets of sanctions measures: 1) sanctions targeted at particular activities or sectors in a specific third country, and 2) list-based sanctions targeting individuals and entities, including those connected to such third countries and/or more generally associated with terrorist organizations. Unlike the United States, the EU does not impose comprehensive economic sanctions programs against third countries and its sanctions against Iran, for example, are fairly limited. EU sanctions also generally prohibit the knowing and intentional participation in activities, the object or effect of which is to circumvent the measures imposed by the EU. Individual EU Member States and the UK, while bound by EU sanctions, can also impose their own economic sanctions that go beyond the scope of those of the EU (even if this is rare).

Currently, the EU maintains substantial sanctions programs (i.e., going beyond arms embargoes and list-based sanctions) against Iran, North Korea, Russia, Crimea/Sevastopol and Syria. These restrictions can target trade in specific goods, various activities involving whole sectors of a country's economy (e.g., the EU's sectoral sanctions targeting the Russian financial, oil and gas, and defense sectors) and/or may require notification or authorization of payments to or from parties in a targeted country.

As part of its list-based sanctions, the EU imposes restrictions on certain designated Restricted Parties, such as those designated under EU asset freeze measures maintained by the EU ("EU Asset Freeze"<sup>9</sup>). Under the EU Asset Freeze, all funds and economic resources belonging to, owned, held or controlled by Restricted Parties in the EU are frozen. It is also generally prohibited to make funds or economic resources available, directly or indirectly (i.e., through third parties), to or for the benefit of Restricted Parties. The concepts 'funds' and 'economic resources' are interpreted very broadly to include anything that can be used to obtain funds, goods or services. This means most commercial activities involving Restricted Parties are prohibited, which would include (but is not limited to) any direct or indirect receipt of funds from and payment of funds or supply of goods to such parties. The EU also maintains sector-based sanctions on certain individuals and entities (e.g., certain financial institutions and energy and defense companies in Russia). The targeted parties are specified in the respective EU Regulations imposing sanctions,<sup>10</sup> and the EU does not maintain a consolidated list of parties targeted by these sectoral sanctions.

The EU also has a "Blocking Regulation" in place to protect EU interests from extra-territorial application of certain sanctions imposed by third countries. Under the EU Blocking Regulation, certain individuals and entities connected to the EU (e.g., EU Member State nationals that are EU residents, entities incorporated within the EU, and individuals acting in a professional capacity within the EU) are prohibited from complying, "actively or by deliberate omission", with certain listed foreign sanctions. Currently, such listed foreign sanctions include certain US sanctions targeting Iran and Cuba.

### **3. Export Controls**

---

<sup>9</sup> The EU's consolidated list of persons, groups and entities subject to EU financial sanctions contains the full list in relation to EU Asset Freeze restrictions targeting designated individuals and entities. The EU Asset Freeze restrictions are imposed under numerous Regulations in relation to various EU sanctions regimes, which are frequently amended.

[https://ec.europa.eu/info/business-economy-euro/banking-and-finance/international-relations/sanctions\\_en](https://ec.europa.eu/info/business-economy-euro/banking-and-finance/international-relations/sanctions_en) (requires registration to access). The UK maintains a consolidated list of financial sanctions targets under both EU and UK law.

<https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets>.

<sup>10</sup> See, for example, Council Regulation 833/2014, as amended (imposing sectoral sanctions on certain listed Russian entities in the financial, energy and defense sectors, and certain of their affiliates), available here: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02014R0833-20190709>.

The EU’s dual-use export control regime governs the export out of the EU (i.e., from any of the EU Member States or the UK) of controlled items (including design drawings, manuals, etc.) that could potentially have a military application or which may contribute to the proliferation of Weapons of Mass Destruction (“WMD”). Restricted items listed in the “EU Dual-Use List” (Annex I to Regulation 428/2009), as amended regularly, may not be exported without an export license or prior registration or notification, which must be obtained or made in the competent EU Member State. The EU Dual-Use List is based on various international arrangements and the scope of items is therefore similar, but not identical, to the scope of controlled products and technology under the US EAR. Catch-all provisions may also trigger controls for non-listed items in certain cases involving WMD and related concerns, and certain EU Member States and the UK may apply dual-use controls to additional items on national lists.

Additionally, export licenses are required in the EU for items on the EU’s Common Military List, which is implemented by all EU Member States. Beyond this list, EU Member States and the UK may have additional items on their national lists and they may require licenses for exports of non-listed items supplied to the military or law enforcement authorities under broad catch-all clauses, creating the possibility that military export controls might extend beyond purely military products in certain EU Member States and the UK.

In the UK, the Export Control Act (2002) and the Export Control Order (2008) provide the legal framework for UK export controls applying on top of the EU’s dual-use export regime. The UK Strategic Export Control Lists<sup>11</sup> specify all the so-called “strategic” goods (i.e. dual-use and military items) subject to an export license in the UK.

### **III. SUMMARY OF ANTI-CORRUPTION AND TRADE CONTROL COMPLIANCE PROCEDURES**

The SSW Group maintains internal controls, established in the Anti-Corruption and Trade Control Compliance Procedures, designed to promote compliance with Anti-Corruption and Trade Control Laws and this Policy. These Procedures are drafted in line with OFAC’s Framework for Compliance Commitments and BIS’ Export Compliance Guidelines. See the Anti-Corruption and Trade Control Compliance Procedures for further detail. The Procedures address the following key compliance areas:

- Know Your Customer (“KYC”) diligence:
  - Counterparty<sup>12</sup> and employee compliance screening against all relevant US, EU, UK, UN, and other appropriate sanctions and export control lists, and against various other sources for anti-corruption risk;
  - Anti-Corruption KYC for counterparties who conduct business with Government Officials or Government Entities on the SSW Group’s behalf
  - Review to identify and resolve any compliance “red flags” (common signals that can indicate an individual or entity may present a compliance risk);
  - Know Your Customer’s Customer diligence, as appropriate;

---

<sup>11</sup> The latest consolidated version of the UK Strategic Export Controls Lists is 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>.

<sup>12</sup> Counterparties include any third party the SSW Group does business with, including customers, vendors, financial institutions, consultants, managing directors, and independent contractors.

- Standard Anti-Corruption and Trade Control contract provisions for use in all SSW Group contracts;
- Export control classification and licensing procedures;
- Consultant expense approval guidelines;
- Technology access procedures for any SSW Group technology controlled under applicable export control laws;
- Periodic refreshers of compliance screening and background checks to account for changes in counterparty information or in trade control lists and anti-corruption sources;
- Anti-Corruption and Trade Control training of employees, as appropriate; and
- Compliance testing and audits.

#### **IV. TRAINING AND EMPLOYEE ENGAGEMENT**

Appropriate employees of the SSW Group shall participate in training courses on compliance with applicable Anti-Corruption and Trade Control Laws and ethical business practices adopted by the SSW Group in accordance with the training schedule set by the Company and will certify their participation in the training.

All employees at the time of hiring shall sign a written commitment to comply with the requirements of this Policy.

#### **V. RECORDKEEPING**

**ALL RECORDS RELATING TO ANTI-CORRUPTION OR TRADE CONTROL COMPLIANCE MUST BE RETAINED FOR A MINIMUM OF FIVE YEARS UNLESS THE CCO EXPRESSLY DIRECTS OTHERWISE.**

There are two principal categories of records that must be retained: (1) administrative records such as licenses and internal records generated under the Anti-Corruption and Trade Control Compliance Procedures; and (2) transactional records such as commercial invoices, ITNs (for purposes of accessing AES information), packing lists, and airway bills. Under US Anti-Corruption and Trade Control Laws, these records must be kept for a minimum of five years, and in some cases longer. In other jurisdictions, local laws on record retention or specific record retention conditions stated in any export licenses (including general licenses) will apply, which may feature longer retention periods. After the five-year or other applicable term has expired, the CCO must approve any destruction of anti-corruption or trade control related documents.

#### **IV. REPORTING AND HOW TO ADDRESS POTENTIAL NON-COMPLIANCE OR VIOLATIONS**

Anti-Corruption and Trade Control Laws are complex, and mistakes can happen even when best efforts are used to follow procedures intended to ensure compliance. If you suspect a problem or violation, you have a duty to report the issue and should bring it immediately to the attention of the CCO. See Chapter 8 of the Anti-Corruption and Trade Control Compliance Procedures. It is extremely important that you bring any concern to the CCO's attention immediately, so that we can correct the problem, identify the root cause, and minimize any potentially negative consequences. The SSW Group does not permit retaliation or detrimental treatment of any kind against employees for good-faith concerns submitted under this Policy.

Company Persons must immediately report to the CCO any suspected or actual violation of Anti-Corruption or Trade Control Laws or of this Policy by the SSW Group or any of its officers, directors, or employees, or any other third-party such as agents, business partners, consultants, or others acting on the SSW Group's behalf. To report violations, a Company Person shall report any suspected noncompliance with this Policy to the CCO or using any other Reporting Mechanism described in the *Seven Seas Water Whistleblower Policy* (see Appendix B above). The report describing a potential violation of Anti-Corruption or Trade Control Laws, or this Policy should set forth all of the information that the Company Person knows regarding the allegation or concern. Once a Company Person has made a report, the Company Person has an obligation to update the report as new information comes into his or her possession.

The Company will take steps to prevent the disclosure of the identity of any Company Person who reports a suspected violation of Anti-Corruption or Trade Control Laws or this Policy without his or her permission, unless disclosure is unavoidable during an investigation. *Under no circumstances shall the reporting of any such information or possible violation serve as a basis for any retaliatory actions to be taken against any Company Person making good faith reports.*

If a Company Person violates any Anti-Corruption or Trade Control Laws or any provision of this Policy, or fails to cooperate in implementing this Policy, the Company Person will be subject to disciplinary action, which may include, but not be limited to, suspension, demotion, reduction in pay, reprimand, or termination.

## **V. DUTY TO REPORT**

The duty to report questions, problems, concerns, and suspected violations to the CCO is an ongoing requirement for every SSW Group employee under this Policy. It is the SSW Group's policy to cooperate with formal inquiries by all anti-corruption, sanctions, and export control government agencies. See Chapter 8 of the Anti-Corruption and Trade Control Compliance Procedures. Should an outside party contact you regarding the SSW Group's compliance policy or procedures, you should contact the CCO immediately. Communication with government agencies in an investigative or enforcement context shall be done strictly through the CCO and/or any other employee(s) empowered by the CCO, including outside counsel.

## **VI. ACKNOWLEDGEMENT**

All employees are required to read and sign the following verification statement on an annual basis, using the Company's e-signature platform:

**Employee Acknowledgement:** I have received and read a copy of the Seven Seas Water Anti-Corruption and Trade Control Policy of Seven Seas and understand its contents. I further acknowledge that I agree to comply with the Seven Seas Water Anti-Corruption and Trade Control Policy. I understand that the SSW Group expressly reserves the right to change, modify, or delete its provisions without notice.