SEVEN SEAS WATER GROUP

Water-as-a-Service®

Cyber Security Policy

Effective: December 9, 2022
Revised: December 9, 2022

SEVEN SEAS WATER GROUP
Water-as-a-Service℠

Table of Contents

SEVEN SEAS WATER GROUP
Water-as-a-Service℠

INTRODUCTION and SCOPE

The purpose of this Seven Seas Water Group Cyber Security Policy ("**Cyber Security Policy**") is to set forth the organizational, technical and physical safeguards and controls established by the Seven Seas Water Group[1] (collectively "**SSWG**" or "**Company**"), so as to ensure the security and confidentiality of the Company's information data systems and data. This Cyber Security Policy forms the foundation of the SSWG Cyber Security Program and sets forth the principles for direct managerial decision making and guide all Company Personnel to facilitate secure and responsible business operations and to manage the security of information assets, Company devices, networks and systems, and maintain accountability. Information systems and data held in it are valuable assets and their confidentiality, integrity and availability are vital to our business. The goal of this Cyber Security Policy is to protect these assets from a wide range of external and internal threats, both intentional and unintentional, in order to effectively reduce the risk of a security incident.

This Cyber Security Policy provides the overall SSWG cyber security framework and. This Cyber Security Policy applies to the SSWG and its direct and indirect subsidiaries, and all Company Networks and Systems and Nonpublic Information, in paper or electronic form, that is owned, licensed, received, stored and maintained, processed or otherwise accessible by SSWG or its Employees. Effective security is a team effort involving every SSWG Employee. All employees and contractors are responsible to understand and comply with this Cyber Security Policy. Any persons knowingly violating the Cyber Security Policy will be subject to discipline, up to and including termination.

This Cyber Security Policy is subject to periodic review and update to ensure the cyber security objectives continue to be met and that the Cyber Security Policy complies with all applicable laws, rules and regulatory requirements.

Data Security Committee

All questions regarding the Cyber Security Policy should be addressed to the Data Security Committee which has been designated by SSWG to be the following group of people (or their designees):

Chief Financial Officer,
General Counsel/Chief Compliance Officer
IT Director

[1] The SSWG Group is comprised of Marlin Water Solutions Co. ("Marlin"), Tarpon Water Solutions Ltd ("Tarpon"), Yellowfin Water Solutions Co. ("Yellowfin"), Seven Seas Water Solutions USA LLC ("Seven Seas USA"), and AUC Group, LLC. ("AUC") and their respective direct and indirect affiliates and subsidiaries

The Data Security Committee will be responsible for:

- Initial implementation of the Cyber Security Policy
- Initial and annual Employee Training on the Cyber Security Policy
- Regular testing of the safeguards implemented pursuant to this Cyber Security Policy
- Conducting due diligence on our third-party service providers to ensure their ability to implement and maintain appropriate security measures for the nonpublic information for which we have permitted them access and contractually requiring them to implement and maintain appropriate security measures
- Monitoring our third-party service provider's compliance with their contractual obligations to implement and maintain appropriate security measures.

Definitions

For the purposes of this policy (and not with regard to other SSWG policies) the following definitions apply:

"**Company Property**" means all (i) the Company's Networks and Systems; (ii) computing devices, including portable devices, passwords, and log on credentials; and (iii) the Company's Nonpublic information.

"**Encryption**" means transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.

"**Employee**" means, solely for purposes of this Cyber Security Policy, an individual who has any employment relationship to the Company and all directors, officers, consultants, independent contractors, in each case whether full and part- time, short-term, and volunteers engaged by SSWG.

"**Cybersecurity Event**" means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt, or misuse the Company's Networks and Systems, or information stored on the Company's Networks or Systems.

"**Networks and Systems**" means the resources of the organization for the collection, processing, maintenance, use, sharing, dissemination or disposition of information ("Information System") and the Information System implementation with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers and technical control devices.

"**Nonpublic Information**" means

Business related information the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business operations, or security of the Company;

Personal Information, as defined below;

and Personal Health Data

"Personal Information" means any information that identifies, relates to, describes, is reasonably capable of being associated with or could reasonably be linked, directly or indirectly, with a particular individual or household and is not public information, including, but not limited to the following:

Social security number;

Driver's license number;

Other government issued identification card number;

Date of birth;

Biometric information, e.g., fingerprint, handprint, voiceprint, facial scan, retinal or iris scan or other unique physical representation or digital representation of biometric data used for authentication;

Username or email address in combination with a password or security question and answer that would permit access to an online account;

Financial account number or credit or debit card number, with or without any required security code, access code, personal identification number or password that would permit access to an individual's or resident's financial account;

Protected medical, health, and health insurance information;

Internet network activity information (e.g., web browsing history and mobile application usage);

Location data;

Individual purchasing preferences and behaviors; and

Any inferences drawn from the above; and

Solely with respect to EU data subjects, any information relating to an identified or identifiable natural person, directly or indirectly, including name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

"**Service Provider**" means any person or entity that receives, stores, maintains, processes or otherwise is permitted access to nonpublic information through its provision of services to SSWG.

Administrative Safeguards

STANDARDS FOR PROTECTING NONPUBLIC INFORMATION, NETWORKS AND SYSTEMS FROM INTERNAL AND EXTERNAL THREATS

Risk Assessment

SSWG shall initially and annually:

Identify and assess reasonably foreseeable internal and external risks to the security, confidentiality or integrity of those sources of Nonpublic Information;

Evaluate the Company's existing policies, procedures and security systems and other safeguards in place to control such risks; and

Develop, implement and maintain this Cyber Security Policy, updating and improving as necessary the administrative, technical and physical safeguards in place to minimize such risks and to detect and prevent unauthorized access to or use of Nonpublic Information and security system failures, consistent with industry standards and requirements of applicable law.

Implementation

Take reasonable steps to supervise Service Providers, including to:

(a) consider whether any third-party service provider with access to personal information has the capacity to protect such information in the manner required by applicable law

(b) require by contract that any third-party service provider with access to personal information is applying to such information protective security measures that are at least as stringent as those required by applicable law

(c) provide oversight of third-party service providers, including through questionnaires or audits, as appropriate; Appropriately monitor to ensure that the Cyber Security Policy is operating in a manner reasonably calculated to prevent unauthorized access to, or unauthorized use of, Personal Information; and upgrade information safeguards as necessary to limit risks

Review all security measures at least annually and/or whenever there is a material change in SSWG business practices and/or applicable law that may reasonably implicate the security or integrity of records containing Personal Information

Employee training

SSWG conducts onboarding and trainings at least annually of all Employees about this Cyber Security Policy. We conduct interim training whenever the Cyber Security Policy may be revised in a manner that materially changes the requirements for Employee conduct or protocols for use of SSWG Networks and Systems and Company Property (as defined).

Technical Safeguards

GENERAL EMAIL/INTERNET SECURITY AND USE

General Security

Each Employee, vendor and other person using or accessing SSWG information or information systems must adhere to the following policies and consent to the following:

All Company Property will be used in compliance with this Cyber Security Policy and SSWGs other policies and the U.S. Employee Handbook ("Handbook").

Any Personal Information placed or maintained on Company Property may be accessed, viewed, analyzed and handled pursuant to the terms of this Cyber Security Policy and the

Handbook.

Any attempt to circumvent this Cyber Security Policy or SSWG security Cyber Security Policy statements, procedures, restrictions, and requirements (e.g., disconnecting or tunneling a protocol through a firewall) is strictly prohibited and subject to discipline, up to and including termination.

Unauthorized use, destruction, modification and/or distribution of SSWGs Nonpublic Information or Company Property is prohibited and subject to discipline, up to and including termination.

Access to Nonpublic Information is limited solely to those Employees who are reasonably required to know such information to accomplish a legitimate business purpose or enable SSWG to comply with applicable law.

At the end of the work day, all electronic files and records containing Nonpublic Information must be secured in a manner that is consistent with this Cyber Security Policy's requirements for protecting the security of such information.

All Nonpublic Information in electronic form shall be disposed of in a secure manner.

All users will report any irregularities found in information or information systems immediately upon detection as directed in the section entitled "Reporting Security Concerns" below).

Use of any SSWG information system or dissemination of information in a manner bringing disrepute, damage or ill will against SSWG is not authorized Employees and other users will not attach their own computer or test equipment to Company Property without prior approval of the IT team or its designated representative.

System Security

SSWG System Security Cyber Security Policy provision addresses access control, use of hardware, operating systems, software, servers, and backup requirements for all systems maintained and operated by SSWG.

Exceptions to this Cyber Security Policy must be approved by both the IT Director and the Chief Compliance Officer or his/her designated representative.

All Company Property, and personal devices used to access Company Property that process Nonpublic Information, must have reasonably up-to-date firewall protection and operating system security patches, to maintain the security and integrity of Nonpublic Information.

All Company Property (excluding phones and tablets), and personal devices used to access Company Property that process Nonpublic Information, must install reasonably up-to-date malware protection and reasonably up-to-date patches and virus definitions.

Password System

Please see Password Policy

Desktop Services Security

The SSWG Desktop Services Security Cyber Security Policy provision establishes the authorized and legitimate use of hardware, operating systems, software, LAN, file servers and all other peripherals used to access any SSWG information system:

Employees are required to lock their computers when they are not at their desk.

No software of any kind will be installed onto a Company laptop or desktop computer or other Company device without the approval of the IT team.

Unauthorized copying or distributing of copyrighted software is a violation of Federal Copyright Law and will not be permitted.

Users will not allow non-employees to use any SSWG machine or device without authorization of the IT team.

The following items are Company Cyber Security Policy provisions for security monitoring:

All SSWG systems and network activities will be subject to monitoring by SSWG at its discretion to protect the Company and its assets from malicious activity. Your signature on this Cyber Security Policy and your use of SSWG Networks and Systems constitutes your consent to this monitoring.

Disabling or interfering with virus protection software is prohibited.

Disabling or interfering with logging, auditing or monitoring software is prohibited. All SSWG desktop services will be subject to inventory and inspection.

Security irregularities, incidents, emergencies, and disasters related to SSWG information or systems will be reported to the IT team immediately.

The following is the corporate Cyber Security Policy provision for system usage:

Sabotage, destruction, misuse, or unauthorized repairs is prohibited on SSWG information systems.

All repairs will be authorized and performed by the IT team:

Users will secure electronic media associated with their use of SSWG information and information systems.

Storage, development or the unauthorized use of tools that compromise security (such as password crackers or network sniffers) are prohibited unless expressly authorized in writing by the IT team.

Security Incident

See Security Incident Response Plan

Internet Acceptable Use

Internet access is provided to SSWG employees and other authorized users to conduct SSWG business. While these resources are to be used primarily for SSWG business, the Company recognizes that employees may occasionally utilize Company equipment and systems to access the internet for personal purposes during work hours, but expects such personal activity to be limited. In addition to the provisions in the Handbook, internet use is subject to the terms below.

Internet activities that can be attributed to a SSWG domain address (such as posting to newsgroups, use of chat facilities and participation in mail lists) must not bring disrepute to SSWG or associate SSWG with controversial issues (e.g., sexually explicit materials, harassment, etc.).

Internet use must not have a negative effect on SSWG operations or its public image.

Users will not make unauthorized purchases or business commitments on behalf of SSWG through the internet.

Internet users will make full attribution of sources for materials collected from the Internet. Plagiarism or violation of copyright is prohibited.

All Internet users will immediately notify the IT team of any suspicious activity.

All remote access to the SSWG Networks and Systems through the Internet will be encrypted and authenticated in a manner authorized by the IT team.

Nonpublic information transmitted through Company systems will be encrypted.

Email Security

The SSWG Email Security Cyber Security Policy specifies mechanisms for the protection of information sent or retrieved through email. In addition, the Cyber Security Policy guides representatives of SSWG in the acceptable use of email. For this Cyber Security Policy, email means any computer-based messaging including notes, memos, letters and data files that may be sent as attachments.

Employees and other authorized users are required to adhere to the following Cyber Security Policy provisions. Violators of any Cyber Security Policy provision are subject to disciplinary actions, up to and including termination.

The following items are the corporate Cyber Security Policy provisions for Email Access Controls:

Individual email accounts are intended to be used only by the person to whom they are assigned. Special arrangements can be made to share information between team members. In all other cases, no user is authorized to open or read the email of another without the

express consent of senior management (i.e., CEO, President, CFO or Director of HR) except in instances when it is a required part of the employee's job function.

Email is provided to Employees and other users of SSWGs Networks and Systems for the purpose of conducting SSWG business.

Email will be stored on the system up to a maximum per mailbox as set by the IT department. Mailbox is defined as the combined total of deleted items, inbox, sent items and any user-created email folders. Users will receive a warning message stating that they need to clear out space when their mailbox size approaches the maximum storage limitations. Once a mailbox reaches the maximum storage limits the user will no longer receive incoming messages.

Email is strictly prohibited from being forwarded to your personal email address. Emails that are handled through our organization can contain classified and detailed information about the organization and by forwarding to a non-secure email, such as Google or Yahoo mail, that opens the organization up to malicious actors, exploitations, liability issues, and the potential for sensitive information to be shared.

The maximum size of any individual incoming email message will be 35 MB.

Emails containing company proprietary or confidential information shall not be sent outside the organization unless we have an approved and signed Non Disclosure Agreement (NDA).

Terminated Employees and other terminated users will have all email access immediately blocked unless an exception is made by the Chief Compliance Officer.

Terminated Employees and other terminated users must return Company equipment and all records containing Nonpublic Information to IT before payment of final paycheck.

Terminated Employees and other terminated users will have all new emails automatically forwarded to their supervisor, or their designated representative, for 30 days or longer at the discretion of the supervisor.

The Terminated Employee's and other terminated user's supervisor is responsible for disseminating stored emails to the appropriate party.

The following items are the corporate Cyber Security Policy provisions for Content:

Use of profane, inappropriate, pornographic, slanderous, bullying, harassing, or misleading content in email is prohibited.

Inclusion of confidential or proprietary information in email going outside the organization is prohibited unless the receiving organization has an approved and signed Non-Disclosure Agreement (NDA).

Use of email to spam (i.e., global send, mail barrage) is prohibited. This includes the forwarding of chain letters.

Use of email to communicate sexual or other harassment is prohibited. Users may not include any words or phrases that may be construed as derogatory based on race, color, sex, age, disability, national origin or any other category.

Forging of email content (i.e., identification, addresses) is prohibited. Additionally, email cannot be used with the intention to commit illegal activity.

All outgoing email will automatically include the following statement: "This email is intended solely for the person or entity to which it is addressed and may contain confidential and/or privileged information. Any review, dissemination, copying, printing or other use of this email by persons or entities other than the addressee is prohibited. If you have received this email in error, please contact the sender immediately, and delete the material from your computer."

The following items are the Cyber Security Policy provisions for Usage:

Any email activity that is in violation of Cyber Security Policy statements or that constitutes suspicious or threatening internal or external activity will be reported.

When sending email, users should verify all recipients to whom they are sending the message(s) before sending the message(s).

Be aware that deleting an email message does not necessarily mean it has been deleted from the system.

Confidential information being sent should be Encrypted prior to sending. No confidential information should be sent outside the organization, unless we have a signed and approved NDA (Non Disclosure Agreement).

Monitoring of Company IT Systems and Company Property

Subject to applicable law, the Company may monitor, without notice, activities and uses of company IT systems and Company Property by Company personnel. The purpose of the monitoring is to protect Company IT systems, property and data, and this Cyber Security Policy does not create any privacy rights for you. *You should not have any expectation of privacy in (1) any company IT system; or (2) any messages, communications, information, images or records, personal or otherwise, created or transmitted using company IT systems, irrespective of whether those systems are accessed by Company-issued or personal devices.* This Cyber Security Policy is not intended to restrict communications or actions protected or required by applicable law. The Company may monitor company IT systems and Company Property for any legitimate purpose, including but not limited to the following purposes:

- To detect, investigate and prevent unauthorized intrusions, misuse or damage to company IT systems and Company Property;
- To ensure the efficient operation, management and security of company IT systems and Company Property; To prevent, detect or investigate the commission of a criminal offense or a suspected criminal offense;
- To enforce the Company's policies and procedures;
- To gather information in connection with an investigation by a legal or regulatory body or in connection with a legal claim made by or against the Company; and
- To measure employee productivity and managing performance deficiencies.

VIRUS, HOSTILE AND MALICIOUS CODE SECURITY

The intent of this Cyber Security Policy provision is to better protect SSWGs assets against attack from destructive or malicious programs:

Any public domain, freeware or shareware software will be evaluated by the IT team prior to installation on any Company resource.

No unauthorized software will be downloaded and installed on end user machines without express approval from the IT team.

System users will not execute programs of unknown origin, as they may contain

malicious code or logic. Only licensed and approved software will be used on any

company computing resource.

All licensed software will be write-protected and stored by the IT team.

SSWGs' antivirus software will automatically scan all files introduced into its environment for virus, hostile and malicious code before use.

The IT team will ensure that SSWG obtains and deploys the latest in virus protection and detection tools.

All email and files will be scanned for virus, hostile and malicious code.

The unauthorized development, transfer or execution for virus, hostile and malicious code

is strictly prohibited. All users will report any suspicious occurrences to his/her supervisor

or the IT team immediately.

All Company systems will be protected by a standard virus

protection system. Virus engines and data files will be updated

on at least a monthly basis.

Viruses that are detected on a user's workstation will be reported to the IT team immediately for action and resolution.

Anomalous behaviors of any software program will be reported to the IT team immediately.

PERSONAL EQUIPMENT

Bring Your Own Device (BYOD)

This Cyber Security Policy provision provides guidelines for using personally owned devices and related software for corporate use.

Furthermore, based on the amount of Nonpublic Information Employees work with, SSWG management reserves the right to determine which employees can use personally owned devices and which cannot.

Other than as permitted under the BYOD program, personally owned notebooks, tablets, and desktop computers will not be granted direct physical access to the network.

Employees of SSWG will not use or request Company IT resources in the use, network connectivity or installation of their personally owned equipment.

The following is a list of personally owned devices permitted by SSWG for Company work:

Smart phones and tablets may be used to access company email.

If the employee is within a SSWG location and needing internet access, they may connect to the Guest Network only.

Employees and other users who wish to access SSWG Networks and Systems and other Company Property using their personally owned computing device will not be able to do so. You must use a SSWG issued device.

Device Security

The user should implement the following security practices for personal devices if accessing

company email:

Password protect all personally owned devices

Do not leave personally owned devices unattended

Acceptable Use

This Cyber Security Policy provision provides rules for the acceptable use of personally owned devices on the Company's Networks and Systems and other Company Property.

The Acceptable Use Cyber Security Policy provision applies to all SSWG employees, directors, interns, contractors, vendors, and any other person accessing SSWG information or information systems. Exceptions to this Cyber Security Policy provision must be approved by

the Director of IT.

Employees and other users must follow the same rules when accessing Company Networks (including the Guest Network), Systems and other Company Property from both Companies issued equipment and personally owned devices. When connected to the SSWG network, Employees and other users are prohibited from doing the following:

Using the service as part of violating the law

Attempting to break the security of any computer network or user

Attempting to send junk email or spam to anyone

Attempting to send a massive amount of email to a specific person or system to flood their server

Attempting to send or forward emails containing proprietary and confidential information outside of the organization without an approved and signed Non-Disclosure Agreement (NDA).

Wiping of Company Data

All Company data on personal devices is Company Property. Therefore, SSWG reserves the right to wipe the Company data from user's personally owned device at any time. By signing this Cyber Security Policy and submitting to our BYOD Cyber Security Policy provision, you acknowledge that you understand and accept this Cyber Security Policy and consent to this practice.

You further consent to a full wipe of all Company data on your personally owned device when your employment with the Company is terminated. By signing this Cyber Security Policy and submitting to our BYOD Cyber Security Policy, you acknowledge you understand and accept this Cyber Security Policy and consent to this practice.

Release of Liability and Disclaimer to Users

SSWG hereby acknowledges that the use of personally owned devices in connection with SSWG business carries specific risks for which you, as the end user, assume full liability.

In the case of inspection or litigation, SSWG may request inspection and/or retention of a user's personally owned device. In such circumstances, SSWG, in its discretion may make reasonable accommodations to provide a temporary replacement device until the personal device is returned.

Physical Safeguards

Physical Security

Procedures are in place to ensure that secure areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access. Security perimeters are defined to protect areas that contain information systems.

Access to the SSWG's physical office space is generally controlled by the IT Team and secured

by multiple layers of security, including building security and card access requirements. A list of persons that have key card access to the premises is maintained by [the IT Team]. [The IT Team] also has security cameras that monitor and record access to the premises. Servers are generally stored in a secured room or remote location with access limited to select authorized personnel.

Hard copy documents containing Personal Information will be kept in lockable filing cabinets which shall be kept locked, except where attended by employees with a business need for regular access to such information. Documents containing Personal Information must never be left unattended in public spaces, such as copying rooms, conference rooms, or lobbies.

Reporting Security Concerns

The user agrees to report the following security incidents immediately to the IT team:

If the device is lost or stolen

If the device has been attacked with malware, a virus or any other suspicious attack

Upon notification of a security incident, the IT Team will execute the Incident Response Cyber Security Policy.

Employees must report also report all other violations of this Cyber Security Policy to theIT Director, VP of Human Resources or Chief Compliance Officer immediately upon discovery.

SSWG shall review any potential violations of the Cyber Security Policy that are escalated to Chief Compliance Officer.

SSWG Human Resources Department shall impose appropriate discipline for failures to comply with relevant parts of the Cyber Security Policy.

SSWG may not sanction or retaliate against or intimidate any person for reporting a policy violation to the Chief Compliance Officer.