SELECT WATER SOLUTIONS
Cybersecurity and Data Privacy Policy
(Effective as of April 28, 2022)

Introduction

Cyber-attacks and their implications for data security and privacy are material ESG risks, particularly for companies using personally identifiable information (PII) and protected health information (PHI).

Select Energy Services (the "Company") deploys a variety of security measures to fortify the integrity and continued reliability of our information security. These measures include written policies, intrusion prevention system, employee training, and internal and third-party audits of our security infrastructure.

The Board and Management are engaged in information security/cybersecurity strategies and the review process. Policies, procedures, and communication and training campaigns inform employees of the importance of information security and cybersecurity, potential threats, and appropriate actions.

Electronic Information Security Practices and Procedures

The Company follows practices and procedures designed to ensure that networks, systems and electronic data are maintained in a controlled and secure manner. These procedures may include:

- Maintaining confidential information on protected drives or sites
- Reimaging end user devices that are retired or reallocated to other Employees
- Timely system access termination for employees and contractors who have left the company
- Data backups per documented procedures
- Current patch and release levels as appropriate
- Security precautions for remote system access
- Secure password standards

- Role-based system access
- Cyber security training and awareness program
- Cyber-attack prevention
    - Intrusion prevention tools and practices
    - Endpoint protection systems
    - Network monitoring
    - Mobile managed device security
    - Multi-factor authentication

Physical Information Security Practices and Procedures

Employees are responsible for maintaining the confidentiality of physical records by appropriate means including:

- Not leaving confidential information unattended in conference rooms or other public environments
- Storing the information in a locked and restricted file room so that visitors or Employees without a business need for the information do not inadvertently have access
- Shredding or destroying the information by secured disposal services when disposing of the records in accordance with our data retention policies

Unauthorized Access to Personal Data

The Company is required to protect the personal data of individuals maintained on its data systems or in physical files. Personal data of individuals generally means an individual's name plus one or more of the following for that individual:

- Social security number
- Passport number, Driver's license number or state identification card number

- Account number, credit card number, or debit card number, in combination with any required security code access code or password that would permit access to an individual's financial account

Personal data does not include information that is lawfully made available to the general public from federal, state or local government records.

Employees who become aware of a breach of the security of data systems maintained by the Company or by third-parties on behalf of the Company that resulted in, or that reasonably may have resulted in, the acquisition of the personal data of individuals by an unauthorized person, must notify the General Counsel and Chief Compliance Officer and/or Chief Technology Officer immediately of that breach. The General Counsel will coordinate the investigation and response with the Chief Technology Officer, which may include, where appropriate or required by law, notification of the individual(s) whose data may have been acquired by an unauthorized person.

A breach of the security of data systems does not include the good faith acquisition of personal information by an Employee or agent of the Company or its third-party vendors for the purposes of the Company's or the vendor's business provided that the personal information is not used for or subject to further, unauthorized disclosure.

Defining Non-Public Personal Information

Non-public personal information includes:

- All personally identifiable financial information (including names, addresses, telephone numbers, social security and other tax identification numbers, financial circumstances and income and account balances); and

- Any list, description, or other grouping of customers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available information – e.g., a list of persons (and their publicly listed telephone numbers) who have disclosed assets or wealth in excess of $1,000,000.00.

Policy Statement Regarding Use and Treatment of Confidential Information

No confidential information, including non-public personal information, whatever the source, regarding any customer, may be disclosed to anyone except as follows:

- To other Employees in connection with the Company's business

- To an affiliate, but the affiliate may disclose the information only to the same extent as the Company

- To any person expressly authorized by a customer

- To certain of the Company's outside service providers (including its attorneys, custodians, fund administrators, accountants, brokers and consultants)

- To regulators and others when required by law

- To nonaffiliated third parties with whom the Company has a contractual agreement to jointly offer, endorse or sponsor a financial product or service; and to service and maintain customer accounts including effectuating a transaction. Contracts with nonaffiliated third parties creating a joint marketing or servicing agreement with the Company must contain language prohibiting the disclosure of all non-public personal information by the nonaffiliated third party except as necessary to carry out the purpose of the agreement. The General Counsel reviews relevant contracts for inclusion of the requisite disclosure

Procedures Regarding Disclosure of Non-public Personal Information

- Non-public personal information may not be disclosed to any nonaffiliated third parties unless the party has been previously informed of the disclosure, as required by law

- Non-public personal information may be disclosed to the extent specifically permitted or required under other provisions of law

- Otherwise, there may be no disclosure of that information except pursuant to an express disclosure authorization from the party

Penalties for Violation of Procedures

Any violation of the procedures set forth in this Privacy Policy will subject the violating Employee to disciplinary action, including possible termination of employment.