DATA PROTECTION POLICY

This policy and any associated guidelines applies to all information collected and used by the Company from which citizens of the European Union ("EU") can be identified ("Personal Data") and sets out how the Company will manage such information.

Company personnel are required to read, understand and comply with the terms of this policy when involved in the collection and/or use of Personal Data in the course of their work, regardless of whether the Personal Data relates to past, present or prospective Company personnel or individuals from within customer, supplier and other service provider organizations.

Please contact the Data Protection Task Force with any questions about the operation of this policy or if you have any concerns that this policy is not being or has not been followed at dataprotection@superiorenergy.com

This policy is specifically tailored to the rights and protections afforded to EU citizens, the General Data Protection Regulations ("**GDPR**") and legislation adopted to implement GDPR. It does not override any applicable national data privacy laws and regulations in countries where the Company operates.

The Company reserves the right to amend this policy at any time.

1. TYPES OF PERSONAL DATA AND PROCESSING ACTIVITIES

Company personnel should refer to the Privacy Notice on the Company intranet for a comprehensive description of the type of Personal Data that the Company collects, stores and uses, including special categories of data. Remember that an individual can be directly identified by data alone or indirectly identified by data in combination with other factors or identifiers. The identified EU citizen is referred to as a "**Data Subject**".

Processing is an activity that involves the use of Personal Data. It includes collecting, recording or holding the Personal Data or carrying out any operation or set of operations on the Personal Data including organising, amending, retrieving, disclosing, transferring, erasing or destroying it. Our Privacy Notice provides examples of how the Company may process Personal Data and on what legal basis it is processed and retained.

2. THE PRINCIPLES OF DATA PROTECTION

LAWFULNESS, FAIRNESS AND TRANSPARENCY:

Personal Data is processed lawfully, fairly and in a transparent manner. Any processing we undertake shall fall within one or more of the following permitted legal justifications:

(a) the Data Subject has given his or her consent;
(b) the processing is necessary for the performance of a contract with the Data Subject;
(c) to meet our legal compliance obligations;
(d) to protect the Data Subject's vital interests; and/or
(e) to pursue our legitimate interests.

2. THE PRINCIPLES OF DATA PROTECTION (CONT'D)

Information in respect of how and why we collect Personal Data is provided to all Data Subjects in our Privacy Notice.

PURPOSE LIMITATION

Personal Data is collected for specified, explicit and legitimate purposes and shall not be further processed in a manner that is incompatible with those purposes. We will inform the Data Subject before processing his or her Personal Data for a purpose not provided for in the Privacy Notice.

DATA MINIMIZATION

Personal Data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of the processing.

ACCURACY

Personal Data must be accurate and we will take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

STORAGE LIMITATION

Personal Data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purpose(s) for which the data is processed. The Company gives consideration to legal, accounting, or reporting requirements such as applicable statutes of limitation, regulatory investigations and/or litigation, in determining how long Personal Data is retained for.

INTEGRITY AND CONFIDENTIALITY

We put in place technical and organisational security measures appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Company personnel engaged in processing of Personal Data, whether working on Company premises, remotely, at home or at client sites, and including when processing Personal Data on personal devices, must follow all procedures and technologies in place to maintain security from the point of collection to the point of destruction. Further information can be found in Section 3 of this policy and in our Information Technology Policy, Major Incident Response Plan and Enterprise IT Disaster Recovery Plan, all of which are accessible on the Company intranet.

ACCOUNTABILITY

The Company is responsible for and must be able to demonstrate compliance with the principles of data protection under the GDPR. Our policies, procedures and notices together with any guidelines, training, records and internal audits, evidence our commitment to data protection and the accountability principle.

3. IDENTIFYING AND REDUCING THE RISK OF A DATA PROTECTION BREACH

PRIVACY IMPACT ASSESSMENTS

Company personnel involved in processing Personal Data will carry out a data privacy impact assessment ("**DPIA**") as a matter of routine, prior to implementing a system or project which may impact upon the privacy of the Data Subjects involved due to the nature or scope of the processing activity.

3. IDENTIFYING AND REDUCING THE RISK OF A DATA PROTECTION BREACH (CONT'D)

The process is accessed via the GDPR folder of Sharepoint on the Company intranet. It consists of:

Stage 1. Initial screening questionnaire to identify the need for a DPIA;
Stage 2. Privacy Impact Assessment;
Stage 3. Data flow details and Mapping; and
Stage 4. Risk Identification, Agreed Actions and Sign Off Form.

SHARING PERSONAL DATA WITH THIRD PARTIES

The Company only shares the Personal Data we hold with third parties, including but not limited to service providers and professional advisors, if:

(i) we have a lawful basis for doing so;
(ii) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject;
(iii) our due diligence and any PIA (if necessary) confirms that there are adequate contractual safeguards and data security policies and procedures in place; and
(iv) Personal Data transferred outside of the Company by email is manually encrypted by the processor using the Company provided encryption software, Proofpoint.

SHARING PERSONAL DATA WITHIN THE COMPANY

We may share the Personal Data we hold with another employee, contractor, worker, intern or equivalent within the Superior Energy Services organisation (which includes our ultimate parent and all of its subsidiaries and branches), if:

(i) the recipient has a job-related need to know the information; and
(ii) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject.

Where the internal transfer is by electronic format (i.e., by email, thumb or hard drive) and involves sensitive or confidential Personal Data such as compensation data, health information, grievances, disciplinary or legal/ compliance matters and/or is there is a perceived high risk (i.e, of unauthorised access or potential loss), Company personnel shall ensure that appropriate additional consideration is given to security measures.

TRANSFERRING PERSONAL DATA OUTSIDE OF THE EUROPEAN ECONOMIC AREA

Any transfer of Personal Data on an intra-Company group basis across country borders is managed under the Company's Intra-Group Data Transfer Agreement. This agreement adopts EU model clauses and ensures that a recipient of Personal Data outside of the EEA applies an appropriate level of protection to any Personal Data it imports from the EEA and/or subsequently transfers to a sub-processor outside of the Company group.

MARKETING OUR SERVICES

There is no legitimate basis for undertaking direct marketing activities using the Personal Data of our EU customers under relevant data protection laws. It is therefore Company policy not to process Personal Data for direct marketing purposes, unless explicit written consent is obtained and procedures for recipient "opt-out" available at any time.

4. REPORTING OBLIGATIONS

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so within 72 hours. If you know or suspect that a Personal Data Breach has occurred, you should contact the Data Protection Task Force immediately.

5. EU CITIZENS' REQUEST RIGHTS

Data Subjects have certain rights when it comes to how we handle their Personal Data, including rights of access, correction, erasure, objection and restriction. Section 11 of our Privacy Notice contains further information on these rights. You must immediately forward any Data Subject request you make or receive to the Data Protection Task Force and comply with the Company's Data Subject response process. The process is accessed via the GDPR folder of Sharepoint on the Company intranet.

6. RECORD KEEPING

The Company is responsible for keeping full and accurate records of all our data Processing activities, and will, in addition, keep records of privacy impact assessments, all Data Subject consents, requests and related procedures.

7. TRAINING & AUDIT

We require all Company Personnel to read and understand the Data Protection Policy. In addition, you will be required to undergo training appropriate to your role to enable you to comply with the Company's policies and procedures and relevant data protection law.

ACKNOWLEDGEMENT

I, _____ (name), acknowledge that on _____, I received a copy of Superior's Data Protection Policy for employees, workers and contractors and understand that I am responsible for knowing and abiding by its terms.

Signature: _____

Print Name: _____

Print Position: _____