DATA PROTECTION POLICY

This policy governs how Superior Energy Services (**"Superior," "Company," "we"** or "**our"**) collects, uses, stores, retains, shares and safeguards the Personal Information in its possession. Such Personal Information may relate to past, present or prospective Company personnel.

All Company personnel are required to read, understand and comply with the terms of this policy when involved in the collection and/or Processing of Personal Information in the course of their work. Please contact the Data Protection Office at dataprotection@superiorenergy.com 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.

The Company reserves the right to amend this policy at any time. The most updated version will always be available on the Company's intranet.

---

1. TYPES OF PERSONAL INFORMATION AND PROCESSING ACTIVITIES

In this policy **"Personal Information"** refers to any information that relates to an identified or identifiable individual, including but not limited to information such as name, date of birth, contact information, governmental identifiers, demographic data, financial data, medical data, professional data, educational data, inferences made about the individual and more. **"Sensitive Personal Information"** is a subcategory of Personal Information that requires particularly careful treatment, such as race, religion, sexual orientation, medical data, biometrics, geolocation, and government identifiers.

Company personnel should refer to the Website Privacy Notice and Employee Privacy Notice on the Company intranet for a comprehensive description of the types of Personal Information, including Sensitive Personal Information, the Company collects and processes about various categories of people (e.g., employees, contractors, website visitors, actual and prospective customers, and other individuals who interact with the Company). 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 person is referred to as a **"Data Subject."**

"Processing" includes collecting, recording, using, or holding the Personal Information or carrying out any operation or set of operations on the Personal Information including organising, amending, retrieving, disclosing, transferring, erasing or destroying it.

2. THE PRINCIPLES OF DATA PROTECTION

The Company abides by the following principles of data protection, and expects all employees to abide by these principles when processing Personal Information on behalf of the Company:

Lawfulness, Fairness and Transparency. Personal Information must be processed lawfully, fairly and in a transparent manner. Any processing of Personal Information we undertake shall fall within one or more of the following lawful bases:

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. the processing is necessary to meet our legal compliance obligations;

d. the processing is necessary to protect the Data Subject's vital interests; and/or

e. the processing is necessary to pursue ours, or a third party's legitimate interests, and those legitimate interests are not overridden by the Data Subject's interests or fundamental rights and freedoms.

Information regarding how and why we collect Personal Information, and the legal bases on which we rely, is provided to all Data Subjects in our Website Privacy Notice and Employee Privacy Notice.

Purpose Limitation. Personal Information must be collected for specified, explicit and legitimate purposes and shall not be further processed in a manner that is incompatible with those purposes. The purposes of collection shall be disclosed to the Data Subject in the Website Privacy Notice or Employee Privacy Notice, and we will inform the Data Subject before processing his or her Personal Information for a purpose not already disclosed.

Data Minimization. Personal Information collected shall be adequate, relevant and limited to only the amount and types of Personal Information necessary to fulfil the stated purpose(s) of collection. Moreover, Personal Information shall be kept for only as long as necessary to fulfil the stated purpose(s) of collection. 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 Information is retained for.

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

Integrity and Confidentiality. We put in place appropriate physical, technical and organisational security measures to prevent accidental or unlawful destruction, loss, theft, alteration, disclosure or access of Personal Information in the Company's custody ("Breach"). Company personnel engaged in processing of Personal Information, whether working on Company premises, remotely, at home or at client sites, and including when processing Personal Information on personal devices, must follow all procedures and technological safeguards 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 applicable law. 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. STEPS WE TAKE TO IDENTIFY AND REDUCE PRIVACY RISK

Data Privacy Impact Assessments

Under certain circumstances that may impact the privacy of Data Subjects, Company personnel involved in processing Personal Information will need to carry out a Data Privacy Impact Assessment ("**DPIA**"). Those circumstances include, for example, whenever the Company is considering:

a. Large scale processing of Personal Information relating to many individuals or data types,
b. Combining data to reveal new Personal Information about individuals,
c. Processing Personal Information of vulnerable individuals,
d. Processing Sensitive Personal Information,
e. Using new technologies that may impact privacy (e.g., AI, facial recognition),
f. Employing automated decision-making that may have significant effects on individuals,
g. Systematically monitoring publicly accessible areas (e.g., CCTV),
h. Transferring Personal Information internationally between countries, and/or
i. Processing Personal Information in a way that prevents exercising rights or accessing services.

The process for carrying out a DPIA is detailed in the Data Protection Resources section on the Company intranet. It consists of:

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

Sharing Personal Information within the Company or with Third Parties

The Company only shares Personal Information within the Company (e.g., between employees or contractors) or with third parties outside the Company (e.g., with service providers or professional advisors) if all of the following are true:

a. There is a business-related need to know and share the Personal Information,
b. Superior has a lawful basis for sharing the Personal Information,
c. Sharing aligns with the Privacy Notice provided to the Data Subject,
d. Our due diligence and any DPIA (if necessary) confirms that there are adequate contractual safeguards and data security policies and procedures in place,
e. Where the third party is a processor, a written contract is in place that meets applicable legal requirements,

f. For cross-border transfers, an appropriate legal transfer mechanism is implemented, and

g. Appropriate security measures (e.g., encryption) are applied at all times by the third party.

Personal Information constitutes a type of Restricted Record, per the Company's Data Retention Policy. As such, when handling any document that contains Personal Information, Company personnel shall save, store, transmit, retain, and delete the document strictly in line with the requirements for Restricted Records laid out in the Data Retention Policy.

Transfer of Personal Information within the company but across international borders is either governed by the Company's Intra-Group Data Transfer Agreement ("IGDTA") or based on a regulators' adequacy decision for a given country which supports the international transfer. The IGDTA agreement incorporates regulator-approved model clauses and ensures that all Company entities apply an appropriate level of protection to any Personal Information imported from another entity in another country.

Breach Response and Notice

We have put in place procedures to deal with any suspected Breach of Personal Information. In particular, the Company has developed and regularly tests our Major Incident Response Plan and Enterprise IT Disaster Recovery Plan. We will notify applicable Data Subjects, customers, business partners, regulators, and/or other third parties where we are legally required to do so and within the legally required timeframe in the event of a Breach.

If you know or suspect that a Breach of Personal Information has occurred, you must contact the Data Protection Office immediately at dataprotection@superiorenergy.com.

Privacy Rights Requests

Based on their country or state of residence, Data Subjects may have certain privacy rights when it comes to how their Personal Information is handled by corporations, including Superior. These rights may include, for example:

- Right of access
- Right of correction
- Right of erasure
- Right to object to processing
- Right to restrict processing
- Right to limit processing of Sensitive Personal Information
- Right of data portability
- Right to opt out of sale or sharing
- Right to opt out of automated decision-making technology
- Right to withdraw consent
- Right to be notified of a data breach

- Right of non-discrimination
- Right to appeal

To fulfil our obligation to process such privacy rights requests in an appropriate and timely manner, the Company has developed a system to receive and respond to such requests. First, all such Data Subject requests must be sent to the Data Protection Office using the Data Subject Request(s) Form, which is accessible via the Data Protection Resources section on the Company intranet. Next, upon receipt, the relevant employee in the Data Protection Office will review the request as explained in the form and provide a response accordingly.

Record Keeping

The Company is responsible for keeping full and accurate records of all our data processing activities of Personal Information. As such, we will create and maintain records of all such processing activities, as well as all DPIAs, Data Subject consent logs, privacy rights requests and decisions and related procedures.

Training and Audit

We require all Company personnel to read, understand and comply with the Data Protection Policy. To ensure familiarity and compliance, all personnel will be required to undergo regular training appropriate to your role regarding this Data Protection Policy, the Company's other related policies and procedures and relevant data protection law and obligations.

ACKNOWLEDGEMENT

I, _____ (name), acknowledge that on _____ 20___, 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 and position: **_____**