EMPLOYEE PRIVACY NOTICE

Superior Energy Services and its affiliates (collectively "Superior," "Company," "we" or "our") is committed to protecting the privacy and security of our employees' personal information, in compliance with applicable data privacy laws and our Shared Core Values.

This Employee Privacy Notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with data protection legislation. It also provides information on how we manage data security, data sharing within our organisation and/or to third parties, international transfers of personal data, and similar topics. Lastly, this notice lays out the various privacy rights an individual may have and how those rights can be exercised.

This Employee Privacy Notice applies to all prospective, current or former employees, workers, contractors, volunteers and interns (collectively **"Personnel"**). That said, this notice does not form part of any contract of employment or other contract to provide services.

We may update this Employee Privacy Notice at any time. Your continued employment or contract with Superior following update of the notice constitutes your acceptance of and consent to those updates.

1. TYPES OF PERSONAL INFORMATION WE COLLECT

In this Employee Privacy Notice, "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.
We may collect, store, and use the following categories of Personal Information about Personnel:

General Employee Data

- full name
- title
- gender
- date of birth
- photograph
- marital status and dependants
- function
- contact information
- residential address
- social security details (where permissible by law)
- national insurance number
- copy of driving licence
- tax reference number

- information on absence from work and leave
- health conditions
- body measurements (for PPE)
- working time
- date of hire
- notice period
- nationality
- national ID number (where required, and where permissible by law)
- evidence of right to work or passport data
- next of kin and emergency contact information

Compensation

- Bank details
- salary details
- salary plan
- salary payment frequency
- salary currency
- grade
- job bonus (field work)
- annual incentive details
- long term incentive details

Position Data

- position
- job profile
- business title
- department
- level
- employing company
- reporting structure
- location and region of responsibility

Education Data

- CV
- qualifications
- language abilities
- areas of expertise

- training history
- professional memberships
- honours and awards

Career History Data

- grievance and / or disciplinary records
- work experience
- length of time in role(s) and business(es)
- project and industry experience
- assignments undertaken/ worked on
- performance reviews

Mobility information

- geographic mobility
- assignment type
- preferences regarding mobility
- restrictions regarding mobility

Internal Investigation

- data in emails or other documents which may be relevant to an internal investigation
- information about your use of Company information and communications systems
- swipe card records and other data obtained through electronic means (i.e., CCTV footage)

"Sensitive Personal Information" is a subcategory of Personal Information which requires particularly careful treatment and includes information such as race, religion, political opinions, sexual orientation, biometrics, geolocation, and government identifiers. Superior attempts to minimize the amount of Sensitive Personal Information it collects and asks that you do not send the Company such information unless explicitly solicited. In those cases, we may solicit, collect, store and use the following categories of Sensitive Personal Information about Personnel:

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Information about your health, including any medical condition, health and sickness records
- Genetic information and biometric data
- Information about criminal convictions and offences

2. SOURCES OF PERSONAL INFORMATION

We collect Personal Information about Personnel from a variety of sources throughout the application, recruitment and employment process, including directly from the candidate or sometimes from an employment agency. We may sometimes collect additional information from third parties including former employers, credit reference agencies, background check agencies, or our service providers who collect information about personnel in the course of their employment (e.g., benefits provider, on-premises physical security, data hosting, analytics). We may also collect Personal Information from publicly available sources (e.g., the Internet).

3. HOW WE USE PERSONAL INFORMATION

We will only use your Personal Information as described in this Employee Privacy Noticeand as applicable law allows. In particular, we may use your Personal Information for one or more of the following purposes:

- Making a decision about your recruitment or appointment
- Determining the terms on which you work for us
- Confirming that you are legally entitled to work in your country of employment
- Paying you and, if applicable, deducting tax and National Insurance contributions (or equivalent)
- Providing benefits to you (e.g., pension, medical, death in service benefit, fuel card)
- Administering the contract we have entered into with you
- Business management and planning, including accounting and auditing
- Benchmarking, managing, and reviewing job performance
- Making decisions about salary reviews and compensation
- Assessing qualifications for a particular job or task, including decisions about promotions
- Gathering evidence for possible grievance or disciplinary hearings
- Making decisions about your continued employment or engagement
- Making arrangements for the termination of our working relationship
- Education, training and development requirements
- Handling incidents and legal disputes involving you or other employees, workers and contractors
- Ascertaining your fitness to work
- Managing sickness absence
- Complying with health and safety obligations
- Preventing, identifying and responding to fraud or other illegal actions
- Monitoring use of our IT systems to ensure compliance with Company policies and procedures
- Ensuring network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution

- Conducting data analytics studies to better understand employee retention and attrition rates
- Monitoring equal opportunity programs and metrics

If you fail to provide certain Personal Information when requested, we may not be able to perform under the employment or service contract we have entered into with you (e.g., paying you, providing a benefit) or comply with our legal obligations (e.g., accounting obligations, worker health and safety).

We will only use Personal Information in line with the original purpose(s) for which it was initially collected, and future purposes that are compatible with those original purpose(s). If it becomes evident that we will need to use your Personal Information for an unrelated and incompatible purpose not yet disclosed to you, we will notify you and explain the new purpose and legal basis of processing and/or request your explicit consent where required by applicable law.

We will only collect and use information relating to criminal convictions (a type of Sensitive Personal Information) where the law permits us to. Where appropriate and permitted, we may collect such information as part of the recruitment process or we may be notified of such information in the course of your employment relationship. We may use such information to determine whether to continue the employment relationship and to ensure the legitimate interests of the Company, its other employees and its customers are appropriately managed.

4. HOW WE SHARE PERSONAL INFORMATION

We may occasionally have to share your Personal Information with third parties, including but not limited to our third-party service providers, vendors, suppliers, and/or other entities within the Superior corporate group, pursuant to our contract, business relationship or work-related activity, where required by law or where we have another legal basis. For example, the Company may use a third-party payroll administrator, benefits provider, data host platform, or financial auditor.

All of our third-party service providers and all entities within the Superior corporate group are required to take appropriate security measures to protect Personal Information from unauthorized access, use, modification, or disclosure in line with our corporate policies. We do not allow our third-party service providers to use Personal Information for their own purposes. We only permit them to process Personal Information for specified purposes and in accordance with our instructions.

5. INTERNATIONAL TRANSFER

Due to the international nature of our organization, we may transfer Personal Information we collect about you outside of the country where such information is initially collected to another country for storage or processing, including the United States of America or another country with weaker data protection laws. In this case, any international transfer of Personal Information (whether to another Superior corporate entity or to a third party) is supported where necessary by an appropriate international transfer mechanism, such as the Standard Contractual Clauses (SCC), an international data privacy framework, or an adequacy decision.

More specifically, a transfer of Personal Information on an intra-Company group basis across country borders is lawfully conducted pursuant to the Company's Intra-Group Data Transfer Agreement ("IGDTA") and/or on the basis of an adequacy decision for that country. The IGDTA incorporates regulator-approved SCCs and ensures that a recipient of Personal Information outside of the country of collection applies an appropriate level of protection to any Personal Information it imports from the country of collection.

Transfer of Personal Information across borders to a third party is likewise supported by an appropriate international transfer mechanism, whether that be SCC, international data privacy framework, or adequacy decision. We contractually require each service provider to abide by certain minimum data protection requirements and enforce appropriate limitations and security measures.

6. LAWFUL BASIS

We process Personal Information about Personnel only where we can rely on one or more lawful bases to do so under applicable law. Lawful bases will vary by jurisdiction, but generally include:

- Where processing is necessary to enter into or perform a contract with the individual or their organization (e.g., to provide services, manage the relationship, process payments);
- Where processing is necessary to comply with our legal obligations (e.g., tax, accounting, export controls, health and safety, anti money laundering, lawful requests from authorities);
- Where processing is necessary to pursue our or a third party's legitimate interests (e.g., security, website analytics, business development), provided these interests are not overridden by the individual's interests or fundamental rights and freedoms;
- Where processing is necessary to protect the vital interests of an individual;
- Where processing is necessary for tasks in the public interest or under official authority; and/or
- With the individual's consent (e.g., direct marketing, non essential cookies, biometric data). Where this is the sole relied-upon lawful basis, consent may be withdrawn at any time.

In the limited situations where we collect and process Sensitive Personal Information, we do so only where an additional condition applies under applicable law, such as: explicit consent of the individual; obligations and rights in employment/social security; exercise or defense of legal claims; vital interests where the individual is incapable of consenting; processing of data manifestly made public by the individual; or substantial public interest under applicable law with appropriate safeguards.

7. AUTOMATED DECISION-MAKING

Currently, Superior does not utilize any automated decision-making technology to make decisions about Personnel. We will notify you if this position changes.

8. DATA SECURITY

We have put in place appropriate physical, technical, and organisational security measures to prevent Personal Information in Superior's custody from being accidentally or unlawfully lost, stolen, altered, used, accessed, or disclosed. In addition, we limit access to such Personal Information to only those employees, agents, contractors and other third parties who have a business need to know. They will only process Personal Information on our instructions, and they are subject to a duty of confidentiality.

While we work hard to protect the Personal Information in our custody, no system or method of transmission can ever be said to be 100% secure. We encourage you to practice vigilance, and if you ever have reason to believe Superior data or systems have been compromised, please notify the IT Security Team at ITsecurity@superiorenergy.com or 1.866.435.7703. We have robust procedures to respond to suspected data security breaches and will notify you and any applicable regulator or third party of any suspected or actual breach where we are legally required to do so.

9. DATA RETENTION

We retain Personal Information for only as long as it is needed or permitted in light of the purpose(s) for which it was collected. Examples of the criteria used by Superior to determine how long your information is held include consideration of legal, accounting, or reporting requirements such as applicable statutes of limitation, regulatory investigations and/or litigation.

10. YOUR PRIVACY RIGHTS

Under certain circumstances and depending on your country or state of residence, you may have various privacy rights with respect to your own Personal Information. These rights will vary by jurisdiction, but generally include:

- **Right to access your own Personal Information.** This enables you to request that Superior explain in writing which categories of Personal Data we have collected about you, as well as the purposes of collection and third parties to whom the information has been disclosed. It also enables you to receive a copy of the exact Personal Information we hold about you.
- **Right to correction.** This enables you to ask us to correct any incomplete or inaccurate Personal Information we hold about you.
- **Right to erasure.** This enables you to ask us to delete or remove Personal Information about you from our systems, with some exceptions.
- **Right to object to processing**. Where we are relying on a legitimate interest as our legal basis for processing your Personal Information, this enables you to object to our processing on this ground and request that we halt such processing.
- **Right to restrict processing.** This allows you to ask us to suspend our processing of Personal Information about you, for example if you want us to establish its accuracy or the reason for

processing it.

- **Right to limit processing of Sensitive Personal Information.** Where we process your Sensitive Personal Information, this allows you to request that we only process it for limited necessary business purposes, by clicking this "Limit the Use of My Sensitive Personal Information" link or by emailing the Data Protection Office below.
- **Right to data portability.** This enables you to request that we provide your Personal Information to you or another party in a commonly accessible format such that it can be moved to an alternate platform.
- **Right to opt out of sale or sharing.** This enables you to request that we not "sell" your Personal Information to a third party or "share" it with a third party for the purpose of "cross-contextual behavioral advertising" (i.e., targeted advertising), as those terms are defined under certain U.S. state privacy laws. Superior already does not sell Personal Information of Personnel or share it for the stated purpose, so this right is inapplicable here.
- **Right to opt out of automated decision-making technology.** This enables you to request that we not use solely automated tools to make decisions or conduct profiling about you and instead seek comparable human review or alternative processes. Superior already does not use any automated decision-making technologies, so this right is inapplicable here.
- **Right to withdraw consent.** Where we rely on your consent as our sole legal basis for processing your Personal Information, this enables you to withdraw consent for processing at any time. Withdrawal impacts prospective processing, but not retrospective processing.
- **Right to non-discrimination.** Where you decide to exercise any privacy rights applicable to you, this right prevents us from discriminating against you in retaliation.

If you have questions about or want to exercise any of your applicable privacy rights, please contact the Data Protection Office at dataprotection@superiorenergy.com or access the Data Subject Request(s) Form located on the Data Protection Resources section on the Company intranet.

When you submit your privacy rights request, we may need to request additional specific information to help us confirm your identity and ensure your eligibility to exercise the right. This is another appropriate security measure to ensure that Personal Information is not disclosed to any person who has no right to receive it.

Unless your request is unduly excessive, burdensome or repetitive, you will not have to pay a fee to exercise any of your applicable privacy rights. However, we may deny your request, as applicable and upon justification. If we deny your request and you disagree with our decision, you may have the right to appeal the decision internally to our Data Protection Office or externally to your state Attorney General, supervisory authority (e.g., UK Information Commissioner's Office (ICO), Brazilian National Data Protection Authority (ANPD)), or other data protection regulator. Please contact the Data Protection Office at dataprotection@superiorenergy.com for more information on how to appeal internally or to your respective regulator.

11. DATA PROTECTION OFFICER/COMPLIANCE MANAGER

We have appointed representatives from Superior's Legal/Compliance, HR and IT departments to a Data Protection Council to oversee compliance with this Employee Privacy Notice. If you have any questions about this Employee Privacy Notice or how we handle Personal Information, please contact the Data Protection Office at dataprotection@superiorenergy.com.

12. CHANGES TO THIS PRIVACY NOTICE

We reserve the right to update this Employee Privacy Notice at any time, and will notify you upon substantial updates. We may also notify you in other ways from time to time about the processing of your Personal Information.

ACKNOWLEDGEMENT

I, _____ (name), acknowledge that on _____ 20___, I received a copy of Superior's Employee Privacy Notice for employees, workers and contractors and that I have read and understood it.

Signature: **……..**

Print Name and position: **_____**