PRIVACY POLICY

1. Definitions

1.1. "**Account Information**" means any of the following information, if and to the extent provided by Licensee to Company when Licensee enters into the Agreement: as to Licensee or its employees, names, usernames, phone numbers, mailing/email addresses, credit card numbers, credit balances and billing information, history of transactions, project identification codes, and information described in Section 10 of this Privacy Policy; provided that, Account Information does not include, and this Privacy Policy does not govern, any data or content Licensee uploads, processes, or stores on the Company Services, including any personal information of Licensee's users, customers, or agents.

1.2. "**Affiliate**" has the meaning ascribed to such term in the Agreement.

1.3. "**Atlas**" or "**Company**" means Atlas Sand Company, LLC (d/b/a Atlas Energy Solutions).

1.4. "**Atlas Group**" has the meaning ascribed to such term in the Agreement.

1.5. "**Agreement**" means the Software as a Service (SaaS) Agreement entered into by and between Company and the "Licensee" identified therein in relation to the Atlas Platform and/or Atlas Compass App.

1.6. "**Licensee**" means the Person identified as such in the Agreement. Licensee may also be referred to herein as "**you**" (or other iterations of such word, like "**your**").

1.7. "**Order Form**" has the meaning ascribed to such term in the Agreement (if any).

1.8. "**Party**" means Company or Licensee, individually, and "**Parties**" means Company and Licensee, collectively.

1.9. "**Person**" has the meaning ascribed to such term in the Agreement.

1.10. "**Permitted Purposes**" means any actions: (a) described hereunder or (b) deemed necessary, useful, desirable, or advantageous, in the reasonable discretion of the Company, to perform, effectuate, manage, enhance, and optimize the Agreement, including managing Licensee's account, billing, developing new services, improving existing services, conducting audits, protecting or enforcing Company's rights in relation to the Agreement, and complying with applicable legal and regulatory requirements.

1.11. "**Services**" has the meaning ascribed to such term in the Agreement.

2. Scope; Use of Account Information

This Privacy Policy governs the use and disclosure of Account Information. Company will only use the Account Information for the Permitted Purposes. Company will restrict access to the Account Information to the members of Atlas Group with a need to know same in relation to a Permitted Purpose, and your Account Information will not be shared with any party outside of Atlas Group. Further, Company will not disclose, access, sell, share, or use the Account Information except in service of a Permitted Purpose.

3. A Special Note About Minors

Company does not knowingly collect personal information from children under the age of 13. If the Account Information includes personal information relating to a child under 13 without parental

or guardian consent, the parent or guardian may contact Company at contracts@atlas.energy. Company will remove the information.

4. Personal Information Company Collects from You

When you request any of the Services (whether as an informal inquiry or via an Order Form), you may be asked to provide Account Information.

Company uses such Account Information for the Permitted Purposes, which include:

- Sending you information about the Services and/or updating you on any changes to the Services or their capabilities;
- Providing updates regarding any changes to the Agreement (including the terms of this Privacy Policy);
- Responding to an inquiry or request for information; and/or
- Communicating with you about customer-service, account, or invoicing issues.

Company does not restrict the ways in which Company uses (a) non-personal information, such as deidentified data or pseudonymous data or (b) public information.

5. Your Privacy Rights and How to Control Your Information

You may contact Company at contracts@atlas.energy to exercise your privacy rights. You have multiple privacy rights, subject to applicable law, with respect to the personal information Company processes about you:

- Confirm whether Company is processing your personal information.
- Opt out of Company's use or sharing of your personal information and sensitive personal information. You may withdraw your consent you have previously provided for the processing of personal information about you.
- Delete personal information. You can ask Company to erase or delete all or some of the information about you.
- Change or correct personal information. You can edit some of the information about you. You can also ask Company to change, update, or fix information about you in certain cases if it is inaccurate.
- Object to, limit, or restrict use of personal information if: (a) Company lacks the legal right to keep using it or (b) the information is inaccurate.
- Access your information. You can also ask Company for a copy of information about you if you reside in the EU, California or other jurisdictions that provide you with this right as a matter of law.

Notwithstanding anything to the contrary herein, if any request or demand by Licensee Group limits or impairs Company's ability to provide the Services and/or fulfill its obligations under the Agreement (as determined in Company's reasonable discretion), such request shall be deemed a breach of the Order Form(s) and/or Agreement for which the information is necessary, entitling Company to terminate same and exercise any other rights described thereunder.

6. Users Outside the United States

Company is headquartered in the United States of America, and information is processed globally as necessary in accordance with this Privacy Policy. Account Information may thus be accessed by Company or transferred to Company in the United States.

By providing Company with Account Information, you consent to the storage or processing of the Account Information in the United States and acknowledge that the Account Information will be subject to the laws of the United States, including the ability of governments, courts, or law enforcement or regulatory agencies of the United States to obtain disclosure of the Account Information.

7. Legal Basis for Processing in certain Foreign Jurisdictions

For Account Information collected about you in the EU, EEA, the UK and other relevant jurisdictions where disclosure of the legal basis for processing may be required, Company's legal bases for processing the Account Information include:

- Performance of a contract with you when Company provides and maintain the Services. When Company processes Account Information solely to provide the Services to you, this information is necessary to be able to provide the Services. If you do not provide this information, Company may not be able to provide the Services to you.
- Company's legitimate interests in protecting the Services from abuse, fraud, or security risks, or in developing, improving, or promoting the Services, including if/when Company trains its models. This may include the processing of Account Information to communicate adequately with you, to respond to your requests, and to tailor marketing and sales activities to your interests.
- Your consent when Company asks for your consent to process your Account Information for a specific purpose that Company communicates to you. You have the right to withdraw your consent at any time.
- Compliance with legal obligations when Company uses Account Information to comply with applicable law or when Company protects its Affiliates', users', or third parties' rights, safety, and property.
- In order to comply with applicable laws and regulations, such as to comply with a subpoena or other legal process, or to process an opt-out request.

Where required, Company will use appropriate safeguards for transferring Account Information outside of certain countries. Company will only transfer Account Information pursuant to a legally valid transfer mechanism.

You can contact Company at contracts@atlas.energy for matters related to Account Information processing, including to appeal an adverse decision from Company regarding a request under this Privacy Policy. Notwithstanding anything to the contrary herein, if any request or demand by Licensee Group limits or impairs Company's ability to provide the Services and/or fulfill its obligations under the Agreement (as determined in Company's reasonable discretion), such request shall be deemed a breach of the Order Form(s) and/or Agreement for which the information is necessary, entitling Company to terminate same and exercise any other rights described thereunder.

8. How Company Secures Your Information

Company has multiple security measures in place to ensure the confidentiality and protection of the Account Information. The data is stored behind Company's firewall, and the data is encrypted. Company has security measures in place to protect against the loss, misuse, or alteration of Account Information. As with any transmission over the Internet, there is some element of risk involved in sending personal or company information. To minimize this risk, Company encrypts Account Information using the Secure Sockets Layer (SSL) protocol.

9. Data Retention

Company may retain your Account Information for as long as it is reasonably necessary for a legitimate business purpose, including any of the Permitted Purposes. Company may dispose of or delete any such Account Information at any time, except as set forth in any other agreement or document executed by a duly authorized representative of each Party concerning the same or as required by law.

10. Use of Internet Technology ("Cookies" And Log Files)

"Cookies" are bits of information that a website transfers to your computer's hard drive for tracking or recordkeeping purposes. Cookies are used by thousands of websites to make your life as a web user much easier. Company may use third-party tracking cookies, from vendors such as Google, to track anonymous traffic data.

Company gathers information for its log files such as Internet Protocol (IP) address, browser type, Internet Service Provider (ISP), type of computing device, referring and exit pages, platform type, date and time stamp, number of clicks while onsite, and other variables.

Log-file information is not linked to any personally identifiable information and is used only to administer systems, to make improvements to the website, and to ensure communications with users.

11. Third Party Vendors

Company may use third-party vendors, including Google, Microsoft AdCenter, to show ads on other websites on the Internet. Some of these vendors, including Google, may use cookies to serve ads based on a user's prior visits to the Atlas website. Users may opt out of Google's cookies by visiting the Google Adverting Opt-Out Page or the Network Advertising Initiative Opt-Out Page.

12. Links To Outside Sites

Company's website contains links to other websites. While these websites might be of interest to you, please note that their privacy policies may differ from this Privacy Policy. Company encourages you to read the privacy statement of each site you visit.

13. Legal Disclaimer

If required by a court of law or government agency, your Account Information might need to be disclosed, if Company has a good-faith belief that such action is necessary to comply with a current judicial proceeding, a court order, a legal process, or discovery request. Company will take reasonable steps to protect your Account Information. Company will attempt to notify you in

advance so that you can take legal action on your own, if desired, to protect the Account Information.

14. Modifications of this Privacy Policy

From time to time, Company may revise its Privacy Policy, the latest revision of which is available at https://www.atlas.energy/saas-overview-and-terms#privacypolicy. Accordingly, please visit that site periodically to review any revisions.

15. Miscellaneous

Article VII of the Agreement shall apply to this Privacy Policy as if set forth in full herein, *mutatis mutandis*.

DATA PROCESSING AGREEMENT

1. DEFINITIONS

1.1. "**Affiliate**" has the meaning ascribed to such term in the Agreement.

1.2. "**Agreement**" means the Software as a Service (SaaS) Agreement entered into by and between Company and the "Licensee" identified therein in relation to the Atlas Platform and/or Atlas Compass App.

1.3. "**Atlas**" or "**Company**" means Atlas Sand Company, LLC (d/b/a Atlas Energy Solutions).

1.4. "**Company Group**" has the meaning ascribed to such term in the Agreement.

1.5. "**Cloud Service**" means any distinct, hosted, supported, and operated on-demand solution as set out in the Agreement.

1.6. "**Company Services**" means Cloud Services, Professional Services, or Company Support as set out in the Agreement.

1.7. "**Company Support**" means Company support services as set out in the Agreement and may also be referred to in the Agreement as "Support".

1.8. "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing of Personal Data.

1.9. "**Data Protection Law**" means the applicable legislation protecting the fundamental rights and freedoms of natural persons and their right to privacy with regard to the processing of Personal Data under the Agreement.

1.10. "**Data Subject**" means an identified or identifiable natural person as defined by Data Protection Law.

1.11. "**DPA**" means this Data Processing Agreement.

1.12. "**EU Standard Contractual Clauses**" means the unchanged standard contractual clauses, published by the European Commission, reference 2021/914 or any subsequent final version thereof which will automatically apply.

1.13. "**GDPR**" means the General Data Protection Regulation (EU) 2016/679.

1.14. "**Licensee**" means the Person identified as such in the Agreement.

1.15. "**List of Subprocessors**" means a list of the name, address, and role of each Subprocessor Company uses to provide Company Services.

1.15.1. "**Party**" means Company or Licensee, individually, and "**Parties**" means Company and Licensee, collectively.

1.16. "**Person**" has the meaning ascribed to such term in the Agreement.

1.17. "**Personal Data**" means any information relating to a Data Subject. For the purposes of Cloud Services, Personal Data is a sub-set of Licensee Data (as defined in the Agreement).

1.18. "**Personal Data Breach**" means a confirmed breach of Company's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or unauthorized third-party access to Personal Data for which a Processor is required under Data Protection Law to provide notice to the Controller.

1.19. "**Processor**" means a natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of the Controller, be it directly as processor of a Controller or

indirectly as subprocessor of a processor which processes Personal Data on behalf of the Controller.

1.20. "**Professional Services**" means implementation services, consulting services and/or other related services as set out in the Agreement and may also be referred to in the Agreement as "Custom Services".

1.21. "**Subprocessor**" or **"sub-processor"** means third parties engaged by Company or its Affiliates, in each case, in connection with Company Services to process Personal Data under this DPA.

1.22. "**Third Country**" means any country, organization or territory not acknowledged by the European Union under Article 45 of GDPR as a safe country with an adequate level of data protection.

2. BACKGROUND

2.1. Scope

2.1.1. This DPA is incorporated into and forms part of the Agreement between Company and Licensee and sets forth the terms and conditions related to the processing of Personal Data by Company and its Subprocessors in connection with delivering Company Services.

2.1.2. This DPA applies only to Personal Data which is processed by Company or its Subprocessors on behalf of the Licensee as part of providing Company Services.

2.1.3. Where Company or a Subprocessor makes available non-production environments of Company Services, Licensee shall not store Personal Data in such environments. Non-production environments are not intended for the processing and storage of Personal Data and are excluded from the scope of this DPA.

2.2. Structure

Schedules 1 and 2 are incorporated into this DPA. They set out the agreed subject matter, the nature and purpose of the processing, the type of Personal Data, categories of Data Subjects and the applicable technical and organizational measures.

2.3. Governance

2.3.1. Company acts as a Processor under this DPA. Licensee and those entities that Licensee authorizes to use Company Services under the Agreement act as a Controller or Processor. For the purposes of this DPA, where Licensee acts as Processor, it does so under the instructions of its Controller(s).

2.3.2. Licensee acts as a single point of contact and shall obtain any relevant authorizations, consents, instructions, and permissions for the processing of Personal Data in accordance with this DPA, including, where applicable, approval to use Company as a Processor. Where authorizations, consents, instructions, and permissions are provided by Licensee, these are provided not only on behalf of the Licensee but also on behalf of any other Controller. Where Company informs or gives notice to Licensee, such information or notice is deemed received by those Controllers permitted by Licensee to use Company Services. Licensee shall forward such information and notices to the relevant Controllers.

3. SECURITY OF PROCESSING

3.1. Technical and Organizational Measures

Company has implemented and will apply commercially reasonable technical and organizational measures. Licensee has reviewed the appropriateness of such measures before it enters into an Agreement that incorporates this DPA.

3.2. Changes

3.2.1. Company applies the technical and organizational measures to Company's entire customer base receiving the same Company Services. Company will review and may change the technical and organizational measures at any time without prior notice so long as such changes maintain an overall level of security for Personal Data that is comparable or better and not diminished. For example, new measures may be added or individual measures may be replaced by new measures that serve the same or a similar purpose.

4. OBLIGATIONS

4.1. Instructions from Licensee

Company will process Personal Data only in accordance with documented instructions from Licensee as described in this Section 4. In entering into the Agreement and by using the Company Services, Licensee instructs Company to process Personal Data to provide and support the Company Services as set out in the Agreement (including this DPA). Company will use reasonable efforts to follow any other Licensee instructions, as long as they are technically feasible, do not require changes to the Company Services or cost to provide same, and are in accordance with Data Protection Law. If Company cannot comply with an instruction or is of the opinion that an instruction infringes Data Protection Law, Company will notify Licensee without undue delay.

4.2. Processing on Legal Requirement

Company may also process Personal Data where required to do so by applicable law. In such a case, Company shall inform Licensee of that legal requirement before processing unless that law prohibits such information on important grounds of public interest.

4.3. Personnel

To process Personal Data, Company and its Subprocessors shall only grant access to authorized personnel who have committed themselves to confidentiality. Company and its Subprocessors will regularly train personnel having access to Personal Data in applicable data security and data privacy measures.

4.4. Data Subject Requests and Cooperation

4.4.1. At Licensee's request, Company will reasonably cooperate with Licensee and Controllers in dealing with requests from Data Subjects or regulatory authorities regarding Company's processing of Personal Data or any Personal Data Breach. If Company receives a request from a Data Subject in relation to the Personal Data processed hereunder, Company will promptly notify Licensee (where the Data Subject has provided information to identify the Licensee) and shall not respond to such request itself but instead ask the Data Subject to redirect its request to Licensee.

4.4.2. In the event of a dispute with a Data Subject as it relates to Company's processing of Personal Data under this DPA, the Parties shall keep each other informed and, where appropriate, reasonably cooperate with the aim of resolving the dispute amicably with the Data Subject.

4.5. Personal Data Breach Notification

Company will notify Licensee without undue delay after becoming aware of any Personal Data Breach and provide reasonable information in its possession to assist Licensee to meet Licensee's obligations to report a Personal Data Breach as required under Data Protection Law. Company may provide such information in phases as it becomes available. Such notification shall not be interpreted or construed as an admission of fault or liability by Company.

4.6. Assessments Pursuant to Data Protection Law

If, pursuant to Data Protection Law, Licensee (or its Controllers) are required to perform a data protection impact (or similar) assessment or prior consultation with a regulator, at Licensee's request, Company will provide such documents as Company makes generally available for Company Services (for example, this DPA, the Agreement, or Audit Reports and Certifications (defined below)) to the extent necessary to conduct such data protection impact assessment as determined in Company's reasonable discretion. Any additional assistance shall be mutually agreed by the Parties.

4.7. Records of Processing

Each Party is responsible for its compliance with its documentation requirements, in particular maintaining records of processing where required under Data Protection Law. Each Party shall reasonably assist the other Party in fulfilling its documentation requirements, including providing the necessary information in a manner reasonably requested by the other Party (such as using an electronic system), in order to enable compliance with any obligations related to maintaining records of processing.

5. DATA EXPORT AND DELETION

5.1. Export and Retrieval

If and to the extent Company hosts Personal Data in a Cloud Service, during the applicable subscription term of such Cloud Service and subject to the Agreement, Licensee may export and retrieve its Personal Data in a standard format. Export and retrieval may be subject to technical limitations, in which case Company and Licensee will find a reasonable method to allow Licensee access to Personal Data.

5.2. Deletion

5.2.1. Before the applicable subscription term of the Cloud Service expires, Licensee shall perform one final data export which constitutes a final return of Personal Data from the Cloud Service.

5.2.2. At the end of the Agreement, Company shall delete the Personal Data remaining with Company (if any) to the extent required by Data Protection Law.

6. CERTIFICATIONS AND AUDITS

6.1. Licensee Audit

Licensee may audit Company's compliance with the technical and organizational measures relevant to Personal Data processed by Company ("**Licensee Audit**") on request only if:

(a) Company has not provided evidence of its compliance with the technical and organizational measures ("**Audit Reports and Certifications**");

(b) a Personal Data Breach has occurred;

(c) an audit is formally requested by Licensee's data protection authority; or

(d) Data Protection Law sets out a direct audit right.

6.2. Audit Specifications

6.2.1. Prior to initiating a request for audit, Licensee shall review Company's Audit Reports and Certifications. Licensee Audits shall be performed by Licensee or its independent third-party auditor (reasonably acceptable to Company and excluding any third-party auditor who is either a competitor of Company or its Affiliates or not reasonably qualified). Licensee shall provide at least sixty (60) days' advance notice of any audit unless Data Protection Law requires shorter notice.

6.2.2. The start date, timeframe and scope of any Licensee Audit shall be mutually agreed between the Parties. Unless Data Protection Law requires more frequent audits, the frequency of a Licensee Audit shall not exceed once every twenty-four (24) months.

6.2.3. Company resources to support Licensee Audits shall be limited to a maximum equivalent of one (1) business day. Licensee Audits shall take place during Company's normal business hours, not disrupt Company's normal business operations, and be subject to Company's reasonable confidentiality requirements.

6.2.4. Licensee shall provide any audit report resulting from a Licensee Audit to Company. The results of any Licensee Audit shall be treated as Company's confidential information.

6.2.5. Licensee shall bear Company's reasonable costs of any Licensee-initiated audit unless such audit reveals a material breach by Company of this DPA, then Company shall bear its own expenses of an audit. If an audit determines that Company has breached its obligations under the DPA, Company will promptly remedy the breach at its own cost.

7. SUBPROCESSORS

7.1. Permitted Use

Company is granted a general authorization to subcontract the processing of Personal Data to Subprocessors, provided that:

(a) Company on its behalf shall engage Subprocessors under a written (including in electronic form) contract not in conflict with the terms of this DPA in relation to the Subprocessor's processing of Personal Data. Company shall be liable for any breaches by the Subprocessor in accordance with the terms of the Agreement;

(b) Company will evaluate the security, privacy, and confidentiality practices of a Subprocessor prior to its selection in order to establish that it is capable of providing the level of protection of Personal Data required by this DPA; and

(c) Company provides to Licensee the List of Subprocessors by making it available to Licensee in writing upon Licensee's written request.

7.2. New Subprocessors

Company's use of Subprocessors is at its discretion, provided that:

(a) Company will inform Licensee in advance (in any manner permitted by the Agreement or by posting on its website) of any intended additions or replacements to an existing List of Subprocessors. Such advance notification shall be at least thirty (30) calendar days in respect to Cloud Services and Company Support and five (5) business days in respect to Professional Services (each, a "**Notification Period**").

(b) Licensee may object to a new Subprocessor by notifying Company in writing during the Notification Period explaining the reasonable ground(s) for its objection. Company shall not use a new Subprocessor before the expiration of the Notification Period. If Company does not receive any objection from Licensee during the Notification Period, Licensee is deemed to have accepted the new Subprocessor.

(c) If Licensee objects, Company may choose: (i) not to use the Subprocessor; (ii) to take reasonable measures to remedy Licensee's grounds for its objection and use the Subprocessor; or (iii) if the foregoing options are not possible, use the Subprocessor. Termination shall take effect at any time during the term of the Agreement determined by Licensee in its written termination notice, provided Licensee accepts the use of the proposed Subprocessor until the effective termination date.

(d) If Licensee objects but neither of the options under 7.2.(c)(i) or (ii) are pursued and Company has not received notice of termination, Licensee is deemed to have accepted the new Subprocessor.

(e) Any termination under this Section shall be deemed to be without fault by either Party and shall be subject to the terms of the Agreement.

7.3. Emergency Replacement

Where a prompt replacement is required for security or other similar urgent reasons and the reason for the change is outside of Company's reasonable control, a Subprocessor may be replaced without advance notice by Company. In this case, Company will inform Licensee of the replacement Subprocessor as soon as reasonably practicable following its appointment. Section 7.2 will apply accordingly.

8. INTERNATIONAL PROCESSING

8.1. Conditions for International Processing

Company shall be entitled to process Personal Data, including by using Subprocessors, in accordance with this DPA, outside the country in which the Licensee is located as permitted under Data Protection Law.

8.2. EU Standard Contractual Clauses

Sections 8.3 to 8.4 apply where there is a transfer to a Third Country of Personal Data that is either subject to GDPR or to other Data Protection Law and where any required adequacy means under GDPR or other Data Protection Law can be met by entering into the EU Standard Contractual Clauses, as amended in accordance with Data Protection Law.

8.3. Applicability of EU Standard Contractual Clauses Where Company is Not Located in a Third Country

Where Company is not located in a Third Country and acts as a data exporter, Company (or Company Group on its behalf) has entered into the EU Standard Contractual Clauses with each Third Country Subprocessor as the data importer. Module 3 (Processor to Processor) of the EU Standard Contractual Clauses shall apply to such transfers.

8.4. Applicability of EU Standard Contractual Clauses where Company is Located in a Third Country

8.4.1. Where Company is located in a Third Country, or a country that otherwise requires use of the EU Standard Contractual Clauses, Company and Licensee enter into the EU Standard Contractual Clauses with Licensee as the data exporter and Company as the data importer as follows:

(a) Module 2 (Controller to Processor) shall apply where Licensee is a Controller; and

(b) Module 3 (Processor to Processor) shall apply where Licensee is a Processor. Where Licensee acts as Processor under Module 3 (Processor to Processor) of the EU Standard Contractual Clauses, Company acknowledges that Licensee acts as Processor under the instructions of its Controller(s).

Other Controllers or Processors whose use of Company Services is authorized by Licensee under the Agreement may also enter into the EU Standard Contractual Clauses with Company in the same manner as Licensee in accordance with Section 8.4.1 above. In such case, Licensee enters into the EU Standard Contractual Clauses on behalf of other Controllers or Processors.

8.4.2. Where Licensee is located in a Third Country and is acting as a Processor under Module 2 or Module 3 of the EU Standard Contractual Clauses and Company is acting as Licensee's sub-processor, the respective data exporter shall have the following third-party beneficiary right:

In the event that Licensee has factually disappeared, ceased to exist in law, or has become insolvent (in all cases without a successor entity that has assumed the legal obligations of the Licensee by contract or by operation of law), the respective data exporter shall have the right to terminate the affected Company Service solely to the extent that the data exporter's Personal Data is processed. In such event, the respective data exporter also instructs Company to erase or return the Personal Data.

8.4.3. On request from a Data Subject, Licensee may make available to such Data Subject a copy of Module 2 or 3 of the EU Standard Contractual Clauses entered into between Licensee and Company (including the relevant Schedules attached hereto).

9. MISCELLANEOUS.

9.1. Article VII of the Agreement shall apply to this DPA as if set forth in full herein, *mutatis mutandis*.

Schedule 1 Description of the Processing

This Schedule 1 applies to the Processing of Personal Data under the Agreement and for the purposes of the EU Standard Contractual Clauses and Data Protection Law.

Where Licensee and Company enter into the EU Standard Contractual Clauses, Schedule 1 is incorporated as Annex I of the EU Standard Contractual Clauses.

1. OPTIONAL CLAUSES OF THE EU STANDARD CONTRACTUAL CLAUSES

1.1. The governing law of the EU Standard Contractual Clauses shall be the law of Germany and German courts shall have jurisdiction over any disputes resulting from the EU Standard Contractual Clauses.

1.2. The optional Clause 7 and the option in Clause 11a of the EU Standard Contractual Clauses shall not apply.

1.3. Option 2, General Written Authorization of Clause 9 of the EU Standard Contractual Clauses shall apply in accordance with the notification periods set out in Section 7 of this DPA.

2. LIST OF PARTIES

2.1. Under the EU Standard Contractual Clauses (Section 8.4 of the DPA)

2.1.1. Module 2: Transfer Controller to Processor

Where Licensee is the Controller and Company is the Processor, then Licensee is the data exporter and Company is the data importer.

2.1.2. Module 3: Transfer Processor to Processor

Where Licensee is a Processor and Company is a Processor, then Licensee is the data exporter and Company is the data importer.

3. DESCRIPTION OF TRANSFER AND PROCESSING

3.1. Categories of Data Subjects Whose Personal Data is Transferred or Processed:

Personal Data relates to the following categories of Data Subjects: employees or contractors having Personal Data stored, transmitted to, made available to, accessed, or otherwise processed by the data importer.

3.2. Categories of Personal Data that are Transferred or Processed:

By choosing what to disclose to Company (whether directly, indirectly, or via the Company Services), Licensee determines the categories of data that can be transferred or processed under the Agreement. Personal Data relates to the following categories of data: (a) as to a natural person, the name, phone number, and home address, and (b) as to any Person, financial data such as bank account information and credit or debit card data.

3.3. Special Data Categories (if agreed)

3.3.1. The transferred Personal Data may comprise special categories of personal data set out in the Agreement ("**Sensitive Data**"). Company has applied the Technical and Organizational Measures set out in Schedule 2 to ensure a level of security appropriate to protect Sensitive Data.

3.3.2. Transfer of Sensitive Data may trigger the application of the following additional restrictions or safeguards if necessary to take into consideration the nature of the data and the risk of varying likelihood and severity for the rights and freedoms of natural persons (if applicable):

(a) training of personnel;

(b) encryption of data in transit and at rest; and

(c) system access logging and general data access logging.

3.4. Purposes of Data Transfer and Further Processing; Nature of Processing

3.4.1. For Cloud Services

Personal Data is subject to the following basic Processing activities:

(a) use of Personal Data to set up, operate, monitor, provide, and support the Cloud Service (including operational and technical Support);

(b) continuous improvement of Cloud Service features and functionalities provided as part of the Cloud Service including automation, transaction processing, and machine learning;

(c) provision of Professional Services;

(d) communication to authorized users;

(e) storage of Personal Data in dedicated data centers (multi-tenant architecture);

(f) release, development, and upload of any fixes or upgrades to the Cloud Service;

(g) back up and restoration of Personal Data stored in the Cloud Service;

(h) computer processing of Personal Data, including data transmission, data retrieval, and data access;

(i) network access to allow Personal Data transfer;

(j) monitoring, troubleshooting, and administering the underlying Cloud Service infrastructure and database;

(k) security monitoring, network-based intrusion detection support, and penetration testing; and

(l) execution of instructions from Licensee in accordance with the Agreement.

The purpose of the transfer and processing is to provide and support the Cloud Service. Company and its Subprocessors may support the Cloud Service data centers remotely. Support is provided as described in the Agreement.

3.4.2. For Company Support and Professional Services:

Personal Data is subject to the basic processing activities as set out in the Agreement which may include:

(a) accessing systems containing Personal Data in order to provide Company Support and Professional Services;

(b) use of Personal Data to provide and support the Company Services;

(c) continuous improvement of service features and functionalities provided as part of the Company Services, which may include automation, transaction processing, and machine learning;

(d) storage of Personal Data;

(e) computer processing of Personal Data for data transmission; and

(f) execution of instructions from Licensee in accordance with the Agreement.

3.5. The purpose of the transfer is to provide and support the relevant Company Service. Company and its Subprocessors may provide or support the Company Service remotely.

3.6. Personal Data will be transferred on an ongoing basis for the duration of the Agreement. Personal Data will be retained by Company as set out in Section 5 of the DPA.

3.7. Company will transfer Personal Data to Subprocessors identified in the applicable List of Subprocessors for the duration of the Agreement.

4. COMPETENT SUPERVISORY AUTHORITY

4.1. In respect of the EU Standard Contractual Clauses:

Where Licensee is the data exporter under Module 2 or Module 3, the supervisory authority shall be the competent supervisory authority that has supervision over the Licensee in accordance with Clause 13 of the EU Standard Contractual Clauses.

Schedule 2 Technical and Organizational Measures

These Technical and Organizational Measures describe the applicable technical and organizational measures for the purposes of the EU Standard Contractual Clauses and Data Protection Law. Where Licensee and Company enter into the EU Standard Contractual Clauses, Schedule 2 is incorporated as Annex II of the EU Standard Contractual Clauses.

To the extent that provisioning of Company Service(s) involves an international transfer to which the EU Standard Contractual Clauses apply, the technical and organizational measures describe the measures and safeguards that consider the nature of Personal Data and the risks involved. If local laws affect compliance with EU Standard Contractual Clauses, additional safeguards may be triggered during the transmission and processing of Personal Data in the country of destination (if applicable: encryption of data in transit, encryption of data at rest, anonymization, pseudonymization).

TECHNICAL AND ORGANIZATIONAL MEASURES

The following sections define Atlas Sand Company, LLC's (d/b/a Atlas Energy Solutions) ("Company") current technical and organizational measures. COMPANY may change these at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

1. PHYSICAL ACCESS CONTROL

Unauthorized persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems that process and/or use Personal Data are located.

Measures:

1.1. Company protects its assets and facilities using the appropriate means based on the Company Security Policy

1.2. In general, buildings are secured through access control systems (e.g., smart card access system).

1.3. As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.

1.4. Depending on the security classification, buildings, individual areas and surrounding premises maybe further protected by additional measures. These include specific access profiles, video surveillance, intruder alarm systems and biometric access control systems.

1.5. Access rights are granted to authorized persons on an individual basis according to the System and Data Access Control measures (see Section 2 and 3, below). This also applies to visitor access. Guests and visitors to Company buildings must register their names at reception and must be accompanied by authorized Company personnel.

1.6. Company employees and external personnel must wear their ID cards at all Company locations.

2. SYSTEM ACCESS CONTROL

Data processing systems used to provide the Company Service must be prevented from being used without authorization.

Measures:

2.1. Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Authorizations are managed via defined processes according to the Company Security Policy.

2.2. All personnel access Company's systems with a unique identifier (user ID).

2.3. Company has procedures in place to so that requested authorization changes are implemented only in accordance with the Company Security Policy (for example, no rights are granted without authorization). In case personnel leaves the Company, their access rights are revoked.

2.4. Company has established a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form. In the case of domain passwords, the system forces a password change every three months in compliance with the requirements for complex passwords. Each computer has a password-protected screensaver.

2.5. The Company network is protected from the public network by firewalls.

Technical and Organizational Measures for Company Support and Professional Services

2.6. Company uses up–to-date antivirus software at access points to the Company network (for e-mail accounts), as well as on all file servers and all workstations.

2.7. Security patch management is implemented to provide regular and periodic deployment of relevant security updates. Full remote access to Company's corporate network and critical infrastructure is protected by strong authentication.

3. **DATA ACCESS CONTROL**

Persons entitled to use data processing systems gain access only to the Personal Data that they have a right to access, and Personal Data must not be read, copied, modified or removed without authorization in the course of processing, use and storage
.

Measures:

3.1. As part of the Company Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the Company's Information Classification standard.
3.2. Access to Personal Data is granted on a need-to-know basis. Personnel have access to the information that they require in order to fulfill their duty. Company uses authorization concepts that document grant processes and assigned roles per account (user ID). All Customer Data is protected in accordance with the Company Security Policy.

3.3. All production servers are operated in the Data Centers or in secure server rooms. Security measures that protect applications processing Personal Data a e regularly checked. To this end, Company conducts internal and external security checks and penetration tests on its IT systems.

3.4. Company does not allow the installation of software that has not been approved by Company.

3.5. A Company security standard governs how data and data carriers are deleted or destroyed once they are no longer required.

4. **DATA TRANSMISSION CONTROL**

Except as necessary for the provision of the Company Services in accordance with the relevant Agreement, Personal Data must not be read, copied, modified or removed without authorization during transfer. Where data carriers are physically transported, adequate measures are implemented at Company to provide the agreed-upon service levels (for example, encryption and lead-lined containers).

Measures:

4.1. Personal Data in transfer over Company internal networks is protected according to Company Security Policy.

4.2. When data is transferred between Company and its customers, the protection measures required for data transfer are hereby mutually agreed upon between Company and its customer and included as a part of the Agreement. This applies to both physical and network based data transfer. In any case, the Customer assumes responsibility for any data transfer once it is outside of Company-controlled systems (e.g. data being transmitted outside the firewall of the Company Data Center).

5. **DATA INPUT CONTROL**

It will be possible to retrospectively examine and establish whether and by whom Personal Data have been entered, modified or removed from Company data processing systems.

Measures:

5.1. Company only allows authorized personnel to access Personal Data as required in the course of their duty.

5.2. Company has implemented a logging system for input, modification and deletion, or blocking of Personal Data by Company or its Subprocessors within the Company Service to the extent technically possible.

6. **JOB CONTROL**

Job Control is required to ensure that personal data processed on behalf of others are processed strictly in compliance with the Customer's instructions

Measures:

6.1. Company uses controls and processes to monitor compliance with contracts between Company and its customers, Subprocessors or other service providers.

6.2. As part of the Company Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the Company Information Classification standard.

6.3. All Company employees and contractual Subprocessors or other service providers are contractually bound to respect the confidentiality of all sensitive information including trade secrets of Company customers and partners.

For Support Services, Company customers have control over their remote support connections at all times. Company employees cannot access a customer system without the knowledge and consent of the customer. For Support Services, Company provides a specially designated, secure support ticket facility in which Company provides a special access-controlled and monitored security area for transferring access data and passwords. Company customers have control over their remote support connections at all times. Company employees cannot access a customer on premise system without the knowledge and active participation of the customer.

7. **AVAILABILITY CONTROL**

Personal Data will be protected against accidental or unauthorized destruction or loss.

Measures:

7.1. Company employs regular backup processes to provide restoration of business-critical systems as and when necessary.

7.2. Company uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to protect power availability to the Data Centers.

7.3. Company has defined business continuity plans for business-critical processes;

7.4. Emergency processes and systems are regularly tested.

8. **DATA SEPARATION CONTROL**

Personal Data collected for different purposes can be processed separately.

Measures:
8.1. Company uses appropriate technical controls to achieve Customer Data separation at all times.

8.2. Customer (including its approved Controllers) will have access only to their own Data based on secure authentication and authorization.

8.3. If Personal Data is required to handle a support incident from Customer, the data is assigned to that particular message and used only to process that message; it is not accessed to process any other messages. This data is stored in dedicated support systems.

9. **DATA INTEGRITY CONTROL**

Personal Data will remain intact, complete and current during processing activities.

Measures:

Company has implemented a multi-layered defense strategy as a protection against unauthorized modifications. In particular, Company uses the following to implement the control and measure sections described above. In particular:

9.1. Firewalls;

9.2. Security Monitoring Center;

9.3. Antivirus software;

9.4. Backup and recovery;

9.5. External and internal penetration testing;