EHS INSIGHT GDPR DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") supplements the EHS Insight Terms of Service Agreement available at https://www.ehsinsight.com/tos, as updated from time to time between Customer and StarTex Software, or other agreement between Customer and StarTex governing Customer's use of the Service (the "**Agreement**") when the GDPR applies to your use of the EHS Insight Services to process Customer Data. This DPA is an agreement between you and the entity you represent ("**Customer**", "**you**" or "**your**") and StarTex Software LLC (d/b/a EHS Insight) ("StarTex"). Unless otherwise defined in this DPA or in the Agreement, all capitalized terms used in this DPA will have the meanings given to them in Section 17 of this DPA.

1. Data Processing.

1.1 **Scope and Roles.** This DPA applies when Customer Data is processed by StarTex. In this context, StarTex will act as processor to Customer, who acts as controller of Customer Data.

1.2 **Customer Controls.** Customer can use the Service Controls to assist it with its obligations under the GDPR, including its obligations to respond to requests from data subjects. Taking into account the nature of the processing, Customer agrees that it is unlikely that StarTex would become aware that Customer Data transferred under the Standard Contractual Clauses is inaccurate or outdated. Nonetheless, if StarTex becomes aware that Customer Data transferred under the Standard Contractual Clauses is inaccurate or outdated, it will inform Customer without undue delay. StarTex will cooperate with Customer to erase or rectify inaccurate or outdated Customer Data transferred under the Standard Contractual Clauses by providing the Service Controls that Customer can use to erase or rectify Customer Data.

1.3 **Details of Data Processing.**

1.3.1 **Subject matter.** The subject matter of the data processing under this DPA is Customer Data.

1.3.2 **Duration.** As between StarTex and Customer, the duration of the data processing under this DPA is determined by Customer.

1.3.3 **Purpose.** The purpose of the data processing under this DPA is the provision of the Services initiated by Customer from time to time.

1.3.4 **Nature of the processing.** Facilitate compliance and performance improvement by means of data collection, storage, analysis, and such other Services as described in the Documentation and initiated by Customer from time to time.

1.3.5 **Type of Customer Data.** Customer Data uploaded to the Services under Customer's EHS Insight account.

1.3.6 **Categories of data subjects.** The data subjects could include Customer's customers, employees, suppliers, and End Users.

1.4 **Compliance with Laws**. Each party will comply with all laws, rules, and regulations applicable to it and binding on it in the performance of this DPA, including the GDPR.

2. **Customer Instructions.** The parties agree that this DPA and the Agreement (including Customer providing instructions via configuration tools such as the EHS Insight application and API made available by StarTex for the Services) constitute Customer's documented instructions regarding StarTex's processing of Customer Data ("**Documented Instructions**"). StarTex will process Customer Data only in accordance with Documented Instructions. Additional instructions outside the scope of the Documented Instructions (if any) require prior written agreement between StarTex and Customer, including agreement on any additional fees payable by Customer to StarTex for carrying out such instructions. Customer is entitled to terminate this DPA and the Agreement if StarTex declines to follow instructions requested by Customer that are outside the scope of, or changed from, those given or agreed to be given in this DPA. Taking into account the nature of the processing, Customer agrees that it is unlikely StarTex can form an opinion on whether Documented Instructions infringe the GDPR. If StarTex forms such an opinion, it will immediately inform Customer, in which case, Customer is entitled to withdraw or modify its Documented Instructions.

3. **Confidentiality of Customer Data.** StarTex will not access or use, or disclose to any third party, any Customer Data, except, in each case, as necessary to maintain, provide, or improve the Services, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order). If a governmental body sends StarTex a demand for Customer Data, StarTex will attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, StarTex may provide Customer's basic contact information to the governmental body. If compelled to disclose Customer Data to a governmental body, then StarTex will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless StarTex is legally prohibited from doing so.

4. **Confidentiality Obligations of StarTex Personnel.** StarTex restricts its personnel from processing Customer Data without authorization by StarTex as described in the StarTex Security Standards. StarTex imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.

5. **Security of Data Processing**

5.1 StarTex has implemented and will maintain the technical and organizational measures for the StarTex Network as described in the StarTex Security Standards and this Section. In particular, StarTex has implemented and will maintain the following technical and organizational measures:

(a) security of the StarTex Network as set out in Section 1.1 of the StarTex Security Standards;

(b) physical security of the facilities as set out in Section 1.2 of the StarTex Security Standards;

(c) measures to control access rights for StarTex employees and contractors to the StarTex Network as set out in Section 1.1 of the StarTex Security Standards; and

(d) processes for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures implemented by StarTex as described in Section 2 of the StarTex Security Standards.

5.2 Customer can elect to implement technical and organizational measures to protect Customer Data. Such technical and organizational measures include the following which are described in the Documentation, or as follows industry best practices:

(a) measures to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and services that are operated by Customer;

(b) measures to allow Customer to backup and archive appropriately in order to restore availability and access to Customer Data in a timely manner in the event of a physical or technical incident; and

(c) processes for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures implemented by Customer.

6. Sub-processing.

6.1 **Authorized Sub-processors.** Customer provides general authorization of StarTex's use of sub-processors to provide processing activities on Customer Data on behalf of Customer ("**Sub-processors**") in accordance with this Section. The EHS Insight website (currently posted at https://www.ehsinsight.com/subprocessors/) lists Sub-processors that are currently engaged by StarTex. At least 30 days before StarTex engages a Sub-processor, StarTex will update the applicable website and provide Customer with a mechanism to obtain notice of that update. To object to a Sub-processor, Customer can: (i) terminate the Agreement pursuant to its terms; or (ii) cease using the Service for which StarTex has engaged the Sub-processor.

6.2 **Sub-processor Obligations.** Where StarTex authorizes a Sub-processor as described in Section 6.1:

(i) StarTex will restrict the Sub-processor's access to Customer Data only to what is necessary to provide or maintain the Services in accordance with the Documentation, and StarTex will prohibit the Sub-processor from accessing Customer Data for any other purpose;

(ii) StarTex will enter into a written agreement with the Sub-processor and, to the extent that the Sub-processor performs the same data processing services provided by StarTex under this DPA, StarTex will impose on the Sub-processor the same contractual obligations that StarTex has under this DPA; and

(iii) StarTex will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause StarTex to breach any of StarTex's obligations under this DPA.

7. StarTex Assistance with Data Subject Requests. Taking into account the nature of the processing, the Service Controls are the technical and organizational measures by which StarTex will assist Customer in fulfilling Customer's obligations to respond to data subjects' requests under the GDPR. If a data subject makes a request to StarTex, StarTex will promptly forward such request to Customer once StarTex has identified that the request is from a data subject for whom Customer is responsible. Customer authorizes on its behalf, and on behalf of its controllers when Customer is acting as a processor, StarTex to respond to any data subject who makes a request to StarTex, to confirm that StarTex has forwarded the request to Customer. The parties agree that Customer's use of the Service Controls and StarTex forwarding data subjects' requests to Customer in accordance with this Section, represent the scope and extent of Customer's required assistance.

8. Optional Security Features. StarTex makes available many Service Controls that Customer can elect to use. Customer is responsible for (a) implementing the measures described in Section 5.2,

as appropriate, (b) properly configuring the Services, (c) using the Service Controls to allow Customer to restore the availability and access to Customer Data in a timely manner in the event of a physical or technical incident (for example backups and routine archiving of Customer Data), and (d) taking such steps as Customer considers adequate to maintain appropriate security, protection, and deletion of Customer Data, which includes use of encryption technology to protect Customer Data from unauthorized access and measures to control access rights to Customer Data.

9. Security Incident Notification.

9.1 **Security Incident.** StarTex will (a) notify Customer of a Security Incident without undue delay after becoming aware of the Security Incident, and (b) take appropriate measures to address the Security Incident, including measures to mitigate any adverse effects resulting from the Security Incident.

9.2 **StarTex Assistance.** To enable Customer to notify a Security Incident to supervisory authorities or data subjects (as applicable), StarTex will cooperate with and assist Customer by including in the notification under Section 9.1(a) such information about the Security Incident as StarTex is able to disclose to Customer, taking into account the nature of the processing, the information available to StarTex, and any restrictions on disclosing the information, such as confidentiality. Taking into account the nature of the processing, Customer agrees that it is best able to determine the likely consequences of a Security Incident.

9.3 **Unsuccessful Security Incidents.** Customer agrees that:

(i) an unsuccessful Security Incident will not be subject to this Section 9. An unsuccessful Security Incident is one that results in no unauthorized access to Customer Data or to any of the equipment or facilities utilized by StarTex for storing Customer Data, and could include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents; and

(ii) StarTex's obligation to report or respond to a Security Incident under this Section 9 is not and will not be construed as an acknowledgement by StarTex of any fault or liability of StarTex with respect to the Security Incident.

9.4 **Communication.** Notification(s) of Security Incidents, if any, will be delivered to one or more of Customer's administrators by any means StarTex selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information in the EHS Insight Services and the helpdesk site.

10. StarTex Certifications and Audits.

10.1 **StarTex ISO-Certification and SOC Reports.** In addition to the information contained in this DPA, upon Customer's request, and provided that the parties have an applicable NDA in place, StarTex will make available the certificates issued for the ISO 27001 certification, and the ISO 27017 certification (or the certifications or other documentation evidencing compliance with such alternative standards as are substantially equivalent to ISO 27001 and ISO 27017).

10.2 **SOC Reports and Data Hosting**. StarTex uses Amazon Web Services ("AWS") for hosting the Services, and annually verifies AWS continues to maintain and provide the System and Organization Controls (SOC) 1 Report, the System and Organization Controls (SOC) 2 Report and the System and Organization Controls (SOC) 3 Report (or the reports or other documentation describing the controls implemented by AWS that replace or are substantially equivalent to the SOC 1, SOC 2 and SOC 3). StarTex reserves the right to switch to another hosting vendor so long as the replacement vendor maintains similar controls and reports.

10.3 **StarTex Audits.** StarTex uses external auditors to verify the adequacy of its security measures. This audit: (a) will be performed at least annually; (b) will be performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001; (c) will be performed by independent third party security professionals at StarTex's selection and expense; and (d) will result in the generation of an audit report ("Report"), which will be StarTex's Confidential Information

10.4 **Audit Reports.** At Customer's written request, and provided that the parties have an applicable NDA in place, StarTex will provide Customer with a copy of the Report so that Customer can reasonably verify StarTex's compliance with its obligations under this DPA.

10.5 **Privacy Impact Assessment and Prior Consultation.** Taking into account the nature of the processing and the information available to StarTex, StarTex will assist Customer in complying with Customer's obligations in respect of data protection impact assessments and prior consultation, by providing the information StarTex makes available under this Section 10.

11. Customer Audits. If Customer chooses to conduct any audit, including any inspection, it has the right to request or mandate on its own behalf under the GDPR or the Standard Contractual Clauses, by instructing StarTex to carry out the audit described in Section 10. If Customer wishes to change this instruction regarding the audit, then Customer has the right to request a change to this instruction by sending StarTex written notice as provided for in the Agreement. If StarTex declines to follow any instruction requested by Customer regarding audits, including inspections, Customer is entitled to terminate the Agreement in accordance with its terms.

12. Transfers of Personal Data.

12.1 **Regions.** Customer can specify the location(s) where Customer Data will be processed within the StarTex Network (each a "**Region**"). Once Customer has made its choice, StarTex will not transfer Customer Data from Customer's selected Region(s) except as necessary to provide the Services initiated by Customer, or as necessary to comply with the law or binding order of a governmental body.

12.2 **Application of Standard Contractual Clauses.** Subject to Section 12.3, the Standard Contractual Clauses will only apply to Customer Data that is transferred, either directly or via onward transfer, to any Third Country, (each a "**Data Transfer**").

12.2.1 When Customer is acting as a controller, the Controller-to-Processor Clauses will apply to a Data Transfer.

12.3 **Alternative Transfer Mechanism.** The Standard Contractual Clauses will not apply to a Data Transfer if StarTex has adopted Binding Corporate Rules for Processors or an alternative recognized compliance standard for lawful Data Transfers.

13. **Termination of the DPA.** This DPA will continue in force until the termination of the Agreement (the "**Termination Date**").

14. **Deletion of Customer Data**. At any time up to the Termination Date, and for 90 days following the Termination Date, subject to the terms and conditions of the Agreement, StarTex will delete Customer Data when Customer uses the Service Controls to request such a deletion. No later than the end of this 90-day period, Customer will close the EHS Insight account containing Customer Data.

15. **Duties to Inform.** Where Customer Data becomes subject to confiscation during bankruptcy or insolvency proceedings, or similar measures by third parties while being processed by StarTex, StarTex will inform Customer without undue delay. StarTex will, without undue delay, notify all relevant parties in such action (for example, creditors, bankruptcy trustee) that any Customer Data subjected to those proceedings is Customer's property and area of responsibility and that Customer Data is at Customer's sole disposition.

16. **Entire Agreement; Conflict**. This DPA incorporates the Standard Contractual Clauses by reference. Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between the Agreement and this DPA, the terms of this DPA will control, except that the Service Terms will control over this DPA. Nothing in this document varies or modifies the Standard Contractual Clauses.

17. **Definitions.** Unless otherwise defined in the Agreement, all capitalized terms used in this DPA will have the meanings given to them below:

"**controller**" has the meaning given to it in the GDPR.

"**Controller-to-Processor Clauses**" means the standard contractual clauses between controllers and processors for Data Transfers, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and currently located at https://www.ehsinsight.com/gdpr_c2p_scc.

"**Customer Data**" means all electronic data or information submitted or uploaded by Customer or a User in connection with the Services, which may contain the "personal data" (as defined in the GDPR).

"**EEA**" means the European Economic Area.

"**GDPR**" means Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

"**processing**" has the meaning given to it in the GDPR and "process", "processes" and "processed" will be interpreted accordingly.

"**processor**" has the meaning given to it in the GDPR.

"Security Incident" means a breach of StarTex's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data.

"Service Controls" means the controls, including security features and functionalities, that the Services provide, as described in the Documentation.

"Standard Contractual Clauses" means the Controller-to-Processor Clauses.

"**StarTex Network**" means certain data center facilities, servers, networking equipment, and host software systems (for example, virtual firewalls) that are utilized by StarTex to provide the Services. No physical access is implied by this definition.

"**StarTex Security Standards**" means the security standards attached to the Agreement, or if none are attached to the Agreement, attached to this DPA as Annex 1.

"Third Country" means a country outside the EEA not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR).

Annex 1 StarTex Security Standards

Capitalized terms not otherwise defined in this document have the meanings assigned to them in the Agreement.

1. Information Security Program. StarTex will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) help Customer secure Customer Data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the StarTex Network, and (c) minimize security risks, including through risk assessment and regular testing. StarTex will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:

1.1 Network Security. The StarTex Network will be electronically accessible to employees, contractors, and any other person as necessary to provide the Services. StarTex will maintain access controls and policies to manage what access is allowed to the StarTex Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. StarTex will maintain corrective action and incident response plans to respond to potential security threats.

1.2 Physical Security. Physical components of the StarTex Network are housed in AWS facilities (the "Facilities"). AWS employs physical barrier controls to prevent unauthorized entrance to the Facilities both at the perimeter and at building access points. StarTex maintains no physical facilities for the purpose of hosting Services, and no local networks are connected directly to the StarTex Network.

2. Continued Evaluation. StarTex will conduct periodic reviews of the security of its StarTex Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. StarTex will continually evaluate the security of its StarTex Network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.