STANDARD PERSONAL DATA PROCESSING AGREEMENT

(RELATED TO MASTER AGREEMENT WITH TETRA TECH)

This agreement is dated: *as per the date of the Master Agreement with Tetra Tech.*

PARTIES

(1) **Tetra Tech, Inc.** incorporated and registered in Delaware, USA with company number 2151089 whose main business address is currently at 3475 East Foothill Boulevard, Pasadena, California, CA 91107, and, as applicable, its relevant subsidiary registered in the USA, as specified in the Master Agreement (**Tetra Tech / Customer**); and

(2) The service provider/supplier/contractor/partner/subcontractor or otherwise named party *as specified in the Master Agreement* **(Provider)**.

BACKGROUND

(A) Tetra Tech and the Provider entered into services agreement (**Master Agreement**) on the date of the Master Agreement that may require the Provider to process Personal Data on behalf of Tetra Tech.

(B) Tetra Tech also has subsidiaries/affiliates in the UK and the EEA. This Agreement contains the mandatory clauses required by the GDPR and UKGDPR for contracts between Controllers and Processors (as defined below).

(C) Tetra Tech has also elected to self-certify to the EU-US Data Privacy Framework[1]. For purposes of enforcing compliance with the Data Privacy Framework, Tetra Tech is subject to the investigatory and enforcement authority of the US Federal Trade Commission.

(D) This Personal Data Processing Agreement (**Agreement**) sets out the additional terms, requirements and conditions subject to which the Provider will process Personal Data when providing services under the Master Agreement.

AGREED TERMS

1. Definitions and interpretation

The following definitions and rules of interpretation apply in this Agreement.

1.1 Definitions:

Authorized Persons: the person(s) or categories of person(s) that the Customer authorizes to give the Provider written personal data processing instructions as identified in he Master Agreement as the Customer's contact person(s) or their equivalent and from whom the Provider agrees to accept such instructions.

Business Purposes: the services to be provided by the Provider to the Customer as described in the Master Agreement and any other purpose specifically identified in writing between the parties.

Commissioner: the US Federal Trade Commission and, as applicable for the relevant Personal Data, the UK's Information Commissioner (see Article 4(A3), UK GDPR and section 114, UK's DPA 2018) and/or relevant other EEA data protection authority, as per the applicable Data Protection Legislation.

Controller, Processor, Data Subject, Personal Data, Personal Data Breach and Processing: (save where the context requires otherwise, or as defined in this Agreement) have the meanings given to them in the UK Data Protection Legislation and must be read and interpreted as their equivalent/closest terms available in the US data protection and privacy legislation.

Data Protection Legislation: all data protection and privacy legislation applicable to Tetra Tech and the Provider in force from time to time in the USA, including in the State of California, and, if applicable for processed Personal Data, in the UK/EU including without limitation the UK GDPR and EU GDPR; the UK's Data Protection Act 2018 (and regulations made thereunder) (**DPA 2018**); the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended; and all other legislation and regulatory requirements in force from time to time in the UK/EU which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications); and the guidance and codes of practice issued by the Commissioner or other relevant regulatory authority and which are applicable to a party.

EU GDPR: the General Data Protection Regulation ((EU) 2016/679).

EEA: The European Economic Area, which includes all 27 European Union member states and also Iceland, Liechtenstein and Norway.

Personal Data: means any information relating to an identified or identifiable living individual that is processed by the Provider on behalf of Tetra Tech as a result of, or in connection with, the provision of the services under the Master Agreement; an identifiable living individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

Records: has the meaning given to it in Clause 12.

Standard Contractual Clauses (SCCs): the UK ICO's International Data Transfer Addendum to EU Commission Standard Contractual Clauses and/or the European Commission's Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 as set out in the Annex to Commission Implementing Decision (EU) 2021/914 and/or the European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to processors established in third countries (controller-to-processor transfers), as set out in the Annex to Commission Decision 2010/87/EU as adapted for the UK, a completed copy of which can be found at ANNEX B to this Agreement or such alternative clauses as may be approved by the European Commission or by the UK from time to time.

Term: the term of this Agreement, as defined in Clause 10.

UK GDPR: has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.

[1] The EU-US Data Privacy Framework (including its UK-US extension (**Data Bridge**)) program, as administered by the US Department of Commerce (**Data Privacy Framework** or **DPF**). For more information about the DPF, please see the US Department of Commerce's DPF website located at: *https://www.dataprivacyframework.gov/s/*. To review Tetra Tech's registration and representation on the DPF List, please see the DPF self-certification list located at: *https://www.dataprivacyframework.gov/s/participant-search*.

1.2	**This Agreement is subject to the terms of the Master Agreement and is hereby incorporated into the Master Agreement. Interpretations. Defined terms and rules of interpretation set forth in the Master Agreement apply to the interpretation of this Agreement.**

1.3 The Annexes form part of this Agreement and will have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Annexes.

1.4 A reference to writing or written includes faxes and email.

1.5 In the case of conflict or ambiguity between:

(a) any provision contained in the body of this Agreement and any provision contained in the Annexes, the provision in the body of this Agreement will prevail;

(b) the terms of any accompanying invoice or other documents annexed to this Agreement and any provision contained in the Annexes, the provision contained in the Annexes will prevail;

(c) any of the provisions of this Agreement and the provisions of the Master Agreement, the provisions of this Agreement will prevail; and

(d) any of the provisions of this Agreement and any executed SCCs, the provisions of the executed SCC will prevail.

2. Personal data types and processing purposes

2.1 The Customer and the Provider agree and acknowledge that for the purpose of the Data Protection Legislation:

(a) the Customer is the Controller and the Provider is the Processor.

(b) the Customer retains control of the Personal Data and remains responsible for its compliance obligations under the applicable Data Protection Legislation, including but not limited to providing any required notices and obtaining any required consents, and for the written processing instructions it gives to the Provider.

(c) the Master Agreement describes the subject matter, duration, nature and purpose of the processing and the Personal Data categories and Data Subject types in respect of which the Provider may process the Personal Data to fulfil the Business Purposes.

3. Provider's obligations

3.1 The Provider will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the written instructions from Authorized Persons. The Provider will not process the Personal Data for any other purpose or in a way that does not comply with this Agreement or the Data Protection Legislation. The Provider must promptly notify the Customer if, in its opinion, the Customer's instructions do not comply with the Data Protection Legislation.

3.2 The Provider must comply promptly with any written instruction from Authorized Persons requiring the Provider to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorized processing.

3.3 The Provider will maintain the confidentiality of the Personal Data and will not disclose the Personal Data to third parties unless the Customer or this Agreement specifically authorizes the disclosure, or as required by applicable law, court or regulator (including the Commissioner). If any applicable law, court or regulator (including the Commissioner) requires the Provider to process or disclose the Personal Data to a third party, the Provider must first inform the Customer of such legal or regulatory requirement and give the Customer an opportunity to object or challenge the requirement, unless the applicable law prohibits the giving of such notice.

3.4 The Provider will reasonably assist the Customer, at no additional cost to the Customer, with meeting the Customer's compliance obligations under the Data Protection Legislation, taking into account the nature of the Provider's processing and the information available to the Provider, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with the Commissioner or other relevant regulator (including any relevant Commissioner) under the Data Protection Legislation.

3.5 The Provider must promptly notify the Customer of any changes to the Data Protection Legislation that may reasonably be interpreted as adversely affecting the Provider's performance of the Master Agreement or this Agreement.

3.6 The Provider will only collect Personal Data for the Customer using a notice or method that the Customer specifically pre-approves in writing or as described in the Master Agreement, which contains an approved data privacy notice informing the Data Subject(s) of the Customer's identity and its appointed data protection representative, the purpose or purposes for which their Personal Data will be processed, and any other information that, having regard to the specific circumstances of the collection and expected processing, is required to enable fair processing. The Provider will not modify or alter the notice in any way without the Customer's prior written consent.

4. Provider's employees

4.1 The Provider will ensure that all of its employees:

(a) are informed of the confidential nature of the Personal Data and are bound by confidentiality obligations and use restrictions in respect of the Personal Data;

(b) have undertaken training on the Data Protection Legislation relating to handling Personal Data and how it applies to their particular duties; and

(c) are aware both of the Provider's duties and their personal duties and obligations under the Data Protection Legislation and this Agreement.

4.2 The Provider will take reasonable steps to ensure the reliability, integrity and trustworthiness of all of the Provider's employees with access to the Personal Data.

5. Security

5.1 The Provider must at all times implement appropriate technical and organizational measures against unauthorized or unlawful processing, access, copying, modification, reproduction, display or distribution of the Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data including, but not limited to, the security measures set out in **ANNEX C** and in the Master Agreement (if any). The Provider must document those measures in writing and periodically review them (at least annually) to ensure they remain current and complete.

5.2 The Provider must implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

(a) the pseudonymization and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

(d) a process for regularly testing, assessing and evaluating the effectiveness of the security measures.

6. Personal Data Breach

6.1 The Provider will ***within 24 hours from discovery*** and in any event without undue delay notify the Customer if it becomes aware of:

(a) the loss, unintended destruction or damage, corruption, or unusability of part or all of the Personal Data. The Provider will restore such Personal Data at its own expense as soon as possible.

(b) any accidental, unauthorized or unlawful processing of the Personal Data; or

(c) any Personal Data Breach.

6.2 Where the Provider becomes aware of any situation occurring in clause 6.1 (a), (b) and/or (c) above, it shall, without undue delay, also provide the Customer with the following information:

(a) description of the nature of (a), (b) and/or (c), including the categories of in-scope Personal Data and approximate number of both Data Subjects and the Personal Data records concerned;

(b) the likely consequences; and

(c) a description of the measures taken or proposed to be taken to address situations (a), (b) and/or (c), including measures to mitigate its possible adverse effects.

6.3 Immediately following any accidental, unauthorized or unlawful Personal Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. Further, the Provider will reasonably co-operate with the Customer at no additional cost to the Customer, in the Customer's handling of the matter, including but not limited to:

(a) assisting with any investigation;

(b) providing the Customer with physical access to any facilities and operations affected;

(c) facilitating interviews with the Provider's employees, former employees and others involved in the matter including, but not limited to, its officers and directors;

(d) making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by the Customer; and

(e) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or accidental, unauthorized or unlawful Personal Data processing.

6.4 The Provider will not inform any third party of any accidental, unauthorized, or unlawful processing of all or part of the Personal Data and/or a Personal Data Breach without first obtaining the Customer's written consent, except when required to do so by applicable law.

6.5 The Provider agrees that the Customer has the sole right to determine:

(a) whether to provide notice of the accidental, unauthorized or unlawful processing and/or the Personal Data Breach to any Data Subjects, the Commissioner, other in-scope regulators, law enforcement agencies or others, as required by law or regulation or in the Customer's discretion, including the contents and delivery method of the notice; and

(b) whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

6.6 The Provider will cover all reasonable expenses associated with the performance of the obligations under clause 6.1 to clause 6.3 unless the matter arose directly from the Customer's specific written instructions, negligence, wilful default or breach of this Agreement, in which case the Customer will cover all reasonable proven expenses.

6.7 The Provider will also reimburse the Customer for actual reasonable expenses that the Customer incurs when responding to an incident of accidental, unauthorized or unlawful processing and/or a Personal Data Breach to the extent that the Provider caused such an incident, including all costs of notice and any remedy as set out in clause 6.5.

7. Further transfers of the Customer's Personal Data (within and outside the USA)

7.1 The Provider (and any of its subcontractors) must not transfer or otherwise process the Customer's Personal Data within and outside the USA (**Permitted Area**) without obtaining the Customer's prior written consent.

7.2 Where such consent is granted and when the Personal Data, or part of it, relates to UK or EEA individuals, the Provider may only process, or permit the processing, of the Personal Data outside the Permitted Area under the following conditions:

(a) the Provider is processing the Personal Data in the UK or in the EEA;

(b) the Provider is processing the Personal Data in a territory which is subject to EU/UK adequacy regulations under the Data Protection Legislation that the territory provides adequate protection for the privacy rights of individuals. The Provider must identify in the Master Agreement (or otherwise in writing) the territory that is subject to such adequacy regulations; or

(c) the Provider participates in a valid cross-border transfer mechanism under the Data Protection Legislation, so that the Provider (and, where appropriate, the Customer) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the UK / EU GDPR. The Provider must identify in **Error! Bookmark not defined.**the Master Agreement (or otherwise in writing) the transfer mechanism that enables the parties to comply with these cross-border data transfer provisions and the Provider must immediately inform the Customer of any change to that status; or

(d) the transfer otherwise complies with the Data Protection Legislation for the reasons set out by the Provider in writing or in **Error! Bookmark not defined.**the Master Agreement.

7.3 If any Personal Data transfer between the Customer and the Provider requires **execution of EU Standard Contractual Clauses[2] (SCCs)** in order to comply with the Data Protection Legislation (**where the Customer is the entity exporting UK/EU-related Personal Data to the Provider outside the Permitted Area or within the Permitted Area to a third party that is not certified under the Data Privacy Framework**, the parties will complete all relevant details in, and execute, the SCCs contained in ANNEX B to this Agreement , and take all other actions required to legitimize the transfer.

7.4 If the Customer consents to appointment by the Provider of a subcontractor located outside the Permitted Area or **not certified under the Data Privacy Framework**[3] in compliance with the provisions of clause 8, then the Customer authorizes the Provider to enter into SCCs contained in Annex B with the relevant subcontractor. The Provider will make the executed SCCs available to the Customer on request.

8. Subcontractors

8.1 Other than those subcontractors explicitly named in the Master Agreement, the Provider may not authorize any other third party or subcontractor to process the Personal Data.

8.2 Those subcontractors approved as at the commencement of this Agreement are as set out in the Master Agreement. The Provider must list (or refer to) all approved subcontractors in the Master Agreement and include any subcontractor's name and location and the contact information for the person responsible for privacy and data protection compliance.

8.3 Where the subcontractor fails to fulfil its obligations under the written agreement with the Provider (which must contain terms substantially the same as those set out in this Agreement) the Provider remains fully liable to the Customer for the subcontractor's performance of its agreement obligations.

8.4 The Parties agree that the Provider will be deemed to control legally any Personal Data controlled practically by or in the possession of its subcontractors.

8.5 On the Customer's written request, the Provider will audit a subcontractor's compliance with its obligations regarding the Personal Data and provide the Customer with the audit results. Where the Customer concludes reasonably that the subcontractor is in material default of its obligations regarding the Personal Data, the Customer may in writing instruct the Provider to instruct the subcontractor to remedy such deficiencies within reasonable term, but not longer than fourteen days. If such deficiencies are not remedied within the required term, the Customer may in writing instruct the Provider to stop processing the Personal Data via the relevant subcontractor.

9. Complaints, data subject requests and third-party rights

9.1 The Provider must, at no additional cost to the Customer, take such technical and organizational measures as may be appropriate, and promptly provide such information to the Customer as the Customer may reasonably require, to enable the Customer to comply with:

(a) the rights of Data Subjects under the Data Protection Legislation, including subject access rights, the rights to rectify, port and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and

(b) information or assessment notices served on the Customer by the Commissioner or other relevant US/UK/EU regulator under the Data Protection Legislation.

9.2 The Provider must notify the Customer immediately in writing if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.

9.3 The Provider must notify the Customer within five days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their other rights under the Data Protection Legislation.

9.4 The Provider will give the Customer, at no additional cost to the Customer, its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.

9.5 The Provider must not disclose the Personal Data to any Data Subject or to a third party other than in accordance with the Customer's written instructions, or as required by domestic law.

10. Term and termination

10.1 This Agreement will remain in full force and effect so long as:

(a) the Master Agreement remains in effect; or

(b) the Provider retains any of the Customer's Personal Data related to the Master Agreement in its possession or control (**Term**).

10.2 Any provision of this Agreement that expressly or by implication should come into or continue in force on or after termination of the Master Agreement in order to protect the Personal Data will remain in full force and effect.

10.3 The Provider's failure to comply with the terms of this Agreement shall be considered a material breach of the Master Agreement. In such event, the Customer may terminate the Master Agreement (or any part of the Master Agreement involving the processing of the Personal Data) effective immediately on written notice to the Provider without further liability or obligation of the Customer.

10.4 If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its Master Agreement obligations, the parties may agree to suspend the processing of the Personal Data until that processing complies with the new requirements. If the parties are unable to bring the Personal Data processing into compliance with the Data Protection Legislation, either party may suspend the processing of the Personal Data immediately and terminate the Master Agreement on not less than 30 days' written notice to the other party.

[2] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

[3] Or, in the cases of data transfers within the USA, to any third party that is not certified under the Data Privacy Framework.

11. Data return and destruction

11.1 At the Customer's request, the Provider will give the Customer, or a third party nominated in writing by the Customer, a copy of or access to all or part of the Personal Data in its possession or control in the format and on the media reasonably specified by the Customer.

11.2 On termination of the Master Agreement for any reason or expiry of its term, the Provider will securely delete or destroy or, if directed in writing by the Customer, return and not retain, all or any of the Customer's Personal Data related to this Agreement in its possession or control.

11.3 If any law, regulation, or government or regulatory body requires the Provider to retain any documents or materials or Personal Data that the Provider would otherwise be required to return or destroy, it will notify the Customer in writing of that retention requirement, giving details of the documents, materials or Personal Data that it must retain, the legal basis for retention, and establishing a specific timeline for deletion or destruction once the retention requirement ends.

11.4 The Provider will certify in writing to the Customer that it has destroyed the Personal Data within three days after it completes the deletion or destruction.

12. Records

12.1 The Provider will keep detailed, accurate and up-to-date written records regarding any processing of Personal Data, including but not limited to, the access, control and security of the Personal Data, approved subcontractors, the processing purposes, categories of processing, any transfers of personal data to a third country and related safeguards, and a general description of the technical and organizational security measures referred to in clause 5.1 and 9.1. (**Records**).

12.2 The Provider will ensure that the Records are sufficient to enable the Customer to verify the Provider's compliance with its obligations under this Agreement and the Provider will provide the Customer with copies of the Records upon request.

12.3 The Customer and the Provider must review the information listed in the Annexes to this Agreement at least once a year to confirm its current accuracy and update it when required to reflect current practices.

13. Audit

13.1 The Provider will permit the Customer and its third-party representatives to audit the Provider's compliance with its Agreement obligations, on at least fourteen days' notice, during the Term. The Provider will give the Customer and its third-party representatives all necessary assistance to conduct such audits. The assistance may include, but is not limited to:

(a) physical access to, remote electronic access to, and copies of the Records and any other information held at the Provider's premises or on systems storing the Personal Data;

(b) access to and meetings with any of the Provider's personnel reasonably necessary to provide all explanations and perform the audit effectively; and

(c) inspection of all Records and the infrastructure, electronic data or systems, facilities, equipment or application software used to store, process the Personal Data.

13.2 The notice requirements in clause 13.1 will not apply if the Customer reasonably believes that a Personal Data Breach occurred or is occurring, or the Provider is in breach of any of its obligations under this Agreement or any Data Protection Legislation.

13.3 If a Personal Data Breach occurs or is occurring, or the Provider becomes aware of a breach of any of its obligations under this Agreement or any Data Protection Legislation, the Provider will:

(a) promptly and, in any case, not later than three days of the triggering event, conduct its own audit to determine the cause;

(b) produce a written report that includes detailed plans to remedy any deficiencies identified by the audit;

(c) provide the Customer with a copy of the written audit report; and

(d) remedy any deficiencies identified by the audit within three days.

13.4 At the Customer's written request, the Provider will:

(a) conduct an information security audit before it first begins processing any of the Personal Data and repeat that audit on at least an annual basis;

(b) produce a written report that includes detailed plans to remedy any security deficiencies identified by the audit;

(c) provide the Customer with a copy of the written audit report; and

(d) remedy any deficiencies identified by the audit within fourteen days.

13.5 The Provider will cover all expenses associated with the performance of its obligations under this clause 13.

14. Warranties

14.1 The Provider warrants and represents (having made due and diligent enquiries) that:

(a) it has elected to self-certify to the EU-US Data Privacy Framework[4] or has executed the SCCs in ANNEX B to this Agreement (if established in the USA);

(b) its employees, subcontractors, agents and any other person or persons accessing the Personal Data on its behalf are reliable and trustworthy and have received the required training on the Data Protection Legislation;

(c) it and anyone operating on its behalf will process the Personal Data in compliance with the Data Protection Legislation and other laws, enactments, regulations, orders, standards and other similar instruments;

(d) it has no reason to believe that the Data Protection Legislation prevents it from providing any of the Master Agreement's contracted services; and

(e) it will take appropriate technical and organizational measures to prevent the unauthorized or unlawful processing of Personal Data and the accidental loss or destruction of, or damage to, Personal Data, and ensure a level of security appropriate to:

[4] Including the equivalent UK-US data privacy adequacy framework ("**Data Bridge**")

(i) the harm that might result from such unauthorized or unlawful processing or accidental loss, destruction or damage;

(ii) the nature of the Personal Data protected; and

(iii) comply with all applicable Data Protection Legislation and its information and security policies, including the security measures required in clause 5.1.

14.2 The Customer warrants and represents that the Provider's expected use of the Personal Data for the Business Purposes and as specifically instructed by the Customer will comply with the Data Protection Legislation.

15. Indemnification

15.1 The Provider agrees to indemnify, keep indemnified and defend at its own expense the Customer against all costs, claims, damages or expenses incurred by the Customer or for which the Customer may become liable due to any failure by the Provider or its employees, subcontractors or agents to comply with any of its obligations under this Agreement or the Data Protection Legislation. Any limitation of liability set forth in the Master Agreement will not apply to this Agreement's indemnity or reimbursement obligations.

16. Notice

16.1 Any notice or other communication given to a party under or in connection with this Agreement must be in writing and delivered to:

For the Customer: *As specified in the Customer's Privacy Statement*[5] *and the Master Agreement;*

For the Provider: *As specified in the Master Agreement.*

16.2 This clause 16.1 does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

16.3 A notice given under this agreement is not valid if sent by email, unless such notices are valid under the Master Agreement.

This agreement has been entered into on the date stated at the beginning of it.

Signature and date: The Customer and the Provider agree that execution of the Master Agreement between them or the actual commencement of the services by the Provider, if earlier, shall constitute execution of this Agreement by both parties.

[5] *https://www.tetratech.com/en/privacy-statement#:~:text=We%20will%20not%20trade%2C%20sell,website%20and%20or%20IT%20providers*.

ANNEX A Personal Data Processing Purposes and Details

Subject matter of processing*: as specified in the Master Agreement.*

Duration of Processing: *until the Master Agreement is terminated by either party.*

Nature of Processing: *the nature of the processing means any operation such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) and as further specified in the Master Agreement.*

Business Purposes: *The purpose will include to deliver services under the Master Agreement to the Customer.*

Personal Data Categories: *As specified in the Master Agreement*.

Data Subject Types: *As specified in the Master Agreement.*

Authorized Persons: *As specified in the Master Agreement (parties' contact persons, representatives or equivalent).*

Provider's legal basis for processing Personal Data (outside the UK and the EEA) in order to comply with cross-border transfer restrictions:

a) **Located in a country with a current determination of adequacy** (for Providers in the USA certified under the Data Privacy Framework and other non-UK/EEA countries listed at the European Commission's Adequacy Decisions website at: *https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en*

b) **EU Standard Contractual Clauses and, as applicable, the UK Addendum to the SCCs** (for Providers based in a country without EU's adequacy decision or based in the USA, but not certified under the Data Privacy Framework); Tetra Tech's SCCs are available at: [See Annex B below].]

Approved Subcontractors:

c) All approved subcontractors are listed in the Master Agreement.

ANNEX B Standard Contractual Clauses

TETRA TECH: STANDARD CONTRACTUAL CLAUSES

In the case of transfer of Tetra Tech's Personal Data related to EU/UK Data Subjects to third countries outside the European Economic Area (EEA) and the United Kingdom (UK) (without EU's adequacy decision) under your Master Agreement with Tetra Tech, **the following Standard Contractual Clauses for the transfer of personal data to third countries are considered a mandatory part of and are incorporated into this Agreement:**

Tetra Tech's SCCs published at: *https://intdev.tetratecheurope.com/home/supplier-information/*

ANNEX C SECURITY MEASURES

TECHNICAL AND ORGANISATIONAL MEASURES FOR PROCESSING TETRA TECH'S PERSONAL DATA

As required under the Master Agreement or under the pre-contracting process with Tetra Tech:

- the Provider should be **certified and attested to confirm compliance with the EU-US Data Privacy Framework**[6]. For purposes of enforcing compliance with the Data Privacy Framework, the Provider should be subject to the investigatory and enforcement authority of the Federal Trade Commission; and / or
- the Provider should be certified and attested to confirm compliance with SOC 2[7] standards, by independent auditors (developed by the American Institute of CPAs (AICPA), SOC 2 defines criteria for managing customer data based on five "trust service principles" - security, availability, processing integrity, confidentiality and privacy). Service Organization Controls (SOC) reports must demonstrate its commitment to securing Customer's Personal Data.

As a minimum, the Provider's security program should be designed to:

- Protect the confidentiality, integrity, and availability of Customer's Personal Data in Provider's possession or to which the Provider has access;
- Protect against any anticipated threats or hazards to the confidentiality, integrity, and availability of Customer's Personal Data;
- Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of Customer's Personal Data;
- Protect against accidental loss or destruction of, or damage to, Customer's Personal Data; and
- Safeguard information as set forth in any regulations by which the Provider may be regulated.

The following further describes the **minimum** functions, processes, controls, systems, procedures and measures which the Provider has taken/ should take to ensure the security of the Processing of Tetra Tech's Personal Data under the Master Agreement:

1) TECHNICAL MEASURES TO ENSURE DATA PRIVACY AND PROTECTION

a) Data Protection by Design and Default:

- The Provider takes the requirements of Article 25 UK/EU GDPR into account in the conception and development phase of Customer's purchased product/services development. Processes and functionalities are set up in such a way that the data protection principles such as legality, transparency, purpose limitation, data minimization, etc. as well as the security of processing are considered at an early stage.

b) Encryption

- All personal data processed by the provider must be encrypted, both in transit e.g. Email, and at rest e.g. storage, using industry standard encryption algorithms.
- Storage of personal data on removable media is not permitted unless data is encrypted at rest and with prior approval from the Customer.
- Full disk encryption of endpoint devices processing personal data should be enabled.
- If personal data or confidential information must be transferred to servers which cannot be sent via TLS-encrypted HTTPS uploads, these will be transferred using Secure File Transfer Protocol (SFTP), or other encrypted mechanisms that meet current security industry standards.

c) Data Anonymization

- Where feasible and appropriate the provider anonymizes personal data using techniques such as pseudonymization and hashing so that the personal data cannot be linked to a data subject.

d) Data Masking

- Where access to personal data is required for testing, development or analytical purposes, the provider employs data masking techniques to conceal and protect sensitive data.

e) Access Controls

- Use of authentication methods
  - Access to Personal Data should be facilitated via encrypted protocols: SSH, SSL/ TLS, HTTPS or comparable protocols.
  - A strong and complex password policy should be enforced on all the providers systems processing personal data.
  - Multifactor authentication should be enabled on IT systems and applications where it is supported for both standard user and administrative accounts.

- Device locking in case of inactivity.
  - All devices used by the Provider's employees must have device locking mechanisms in place, which is activated after 15 minutes (or less) of inactivity to prevent unauthorized access to devices and organizational data.

- User Accounts
  - The Provider will have an established account provisioning process, including approvals.
  - All users and administrative accounts are issued with unique usernames and password and must not be shared.
  - The provider will ensure administrator account access is separate from a standard user account. All user accounts not required must be disabled.

[6] Including the equivalent UK-US data privacy adequacy framework ("**Data Bridge**")
[7] https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2

f) End point detection and response technology

- Endpoints and servers that store or process Customer's Personal Data must have end point protection in place.
- Laptops used by the Provider's employees at a minimum are equipped with anti-virus software that is kept up to date.
- Servers should have end point detection and response capability deployed, preferably with a managed detection and response service.
- The Provider should run regular anti malware scans across all the estate.
- The Provider will ensure that a vulnerability management schedule is in place and that all high risk and critical security updates are be remediated in line with vendor provided guidance.

g) Authorization Control

- Authorization controls, such as role-based access will be put in place by the Provider, which includes an approval process. Access to data should be based on the individual's role within the organization and within a system, in order to prevent the processing of personal data by unauthorized persons.
- A formal approval process should be in place when granting administrator access to users.

h) Firewall

- The Provider should have defined firewall rules and policies in place, which includes intrusion detection and prevention capabilities.
- Adopt a default deny approach, where traffic is blocked by default and only explicitly allowed based on defined rules and business justification.
- A Web Application Firewall (WAF) must be used to protect against malicious access attempts on the Internet if Customer's Personal Data is accessible on a web site.

i) Monitoring and Logging

- The Provider should implement a comprehensive logging and monitoring solution which allows the alerting, analysis and recording of network traffic, security events, network anomalies.
- The Provider will retain monitoring logs in line with organizational retention policies.

j) Data Separability

- Ensure that personal data collected is separated from other data and systems in such a way that unplanned use of this data for other purposes is prevented.
- The Provider will ensure there is a separation of development, test and operating environments (as applicable for the services). The Personal Data from the operating environment should only be transferred to test or development environments if it has been made completely anonymous before transfer. The transfer of anonymized data should be encrypted or via a trustworthy network.

k) Separation in networks

- The Provider separates its networks according to the nature of the services defined under the Master Services Agreement and Customer's written instructions. As required for performance of the services for the Customer, the following Provider's networks are used permanently: operating environment ("Production"), test environment ("Staging", "Sandbox"), development environment ("Dev") office IT staff. In addition to these networks, further separate networks are created as required, e.g., for restore tests and penetration tests. Depending on the technical possibilities, the networks are separated either physically or by means of virtual networks.

i) Availability control

- The Provider takes the following steps to ensure that personal data is protected against accidental destruction or loss.
- The Provider will ensure that there is a backup schedule in place, whereby regular automated backups are taken at intervals that align with the organization and customers' needs and data sensitivity The Provider must ensure that its systems in use can be restored in the event of physical or technical failure, including regular tests of the data recovery ("Restore-Tests"), Regular full restore tests are carried out to ensure recoverability in the event of an emergency/disaster.
- Geo-redundancy should be employed where possible to ensure the availability, reliability and disaster recovery capabilities.

m) IT incident management ("Incident Response Management")

- The Provider has a documented procedure for handling security and privacy incidents. This includes the planning and preparation of the response to incidents, procedures for monitoring, detecting and analyzing security-relevant events and the definition of corresponding responsibilities and reporting channels in the event of a violation of the protection of personal data within the framework of the legal requirements.

***

2) ORGANIZATIONAL MEASURES TO ENSURE DATA PRIVACY AND PROTECTION

The Provider has put in place the following organizational measures to ensure the organization operates in a manner that meets data privacy and protection requirements:

a) Organizational Instructions

- The Provider has developed a data governance program including policies, procedures, and guidelines for employees to follow.
- Documentation should include how to identify and manage data privacy issues, best practices for ensuring privacy compliance, and policies for addressing privacy incidents.

b) Commitment to confidentiality and data protection

- The Provider must designate a Data Privacy Officer/ Unit/ Office, as identified on its website, which is tasked with planning, implementing, evaluating and adapt measures in the field of data protection.
- All Provider's employees and contractors are bound in writing to maintain confidentiality and data protection.
- The Provider will ensure that the processing of personal data is in line with its Data Protection policies and all other applicable laws.
- Internal audits on data protection and information security are conducted regularly following recognized industry standards and frameworks.

c) Data protection training

- The Provider's employees and contractors receive regular privacy & security training. Completion rates should be monitored and reported for compliance.

d) Clean Desk Policy

- The Provider has implemented a clean desk policy.
- Employees are instructed to process and store personal data in line with data protection guidelines. Data should only be accessed by those who 'need to know'.
- Physical copies of data containing personal information should be kept to a minimum and only if necessary. This data must be stored in locked cabinets and key management in place.

e) Physical Access Controls

- The Provider must ensure that data is protected in line with its sensitivity and has appropriate physical controls in place to deny unauthorized access to the providers facilities, IT systems used for processing Personal data:
- Opening and Closing office procedures should be in place.
- There must be a controlled distribution of keys which is centrally managed, and procedures are in place to recall or replace keys promptly if needed.

f) Visitor Access Control

- The Provider has a written visitors policy which is implemented throughout its organization. A process should be in place to manage and visitors to the Providers premises, this should include the registration of Visitors, issuing visible Visitor passes, and accompanying the Visitor when accessing more sensitive areas of the premises such as Communication rooms.

g) Business Continuity and Disaster Recovery Recoverability

- The Provider must have a disaster recovery and business continuity plans that ensure the recovery of all systems and restoration of business operations within 48 hours.

h) Review and evaluation measures

- Regular assessments of the effectiveness of the technical and organizational measures should be conducted.

i) Risk Management

- The Provider should have a risk management program for analyzing, evaluating, and allocating risks, and for designing and implementing risk mitigating measures.

3) INDEPENDENT REVIEW OF INFORMATION SECURITY

a) Performance of audits

- Provider's internal audits on data protection and information security are conducted regularly. Audits are carried out following recognized industry standards and frameworks.

b) Review of compliance with security policies and standards

- Provider's compliance with the applicable security guidelines, standards, and other security requirements for the processing of personal data is checked regularly. Where possible, these checks are carried out on a random and unexpected basis.

c) Verification of compliance with technical specifications

- Regular automated and manual vulnerability scans must be performed by the Provider's IT department/support or other qualified authorized personnel to verify the security of the applications and infrastructure, as well as the regular development of the Provider's products/services. Detailed penetration tests should be carried out by an external service provider to specifically examine the applications and infrastructure for vulnerabilities.

d) Supplier Due Diligence

- The Provider adheres to its supplier prequalification process when suppliers may be given access to Customer's Personal Data. This process includes feedback from the Finance and Legal/Privacy Departments/support and incorporates risk assessment, security prequalification and documentation certification steps. Suppliers who will process Personal Data will be required to demonstrate their adherence to applicable data privacy laws, including Article 28 EU/UK GDPR for covered data.
- Protect the confidentiality, integrity, and availability of Customer's Personal Data
- Protect against any anticipated threats or hazards to the confidentiality, integrity, and availability of Customer's Personal Data;
- Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of Customer's Personal Data;
- Protect against accidental loss or destruction of, or damage to, Customer's Personal Data; and
- Safeguard information as set forth in any regulations by which the Provider may be regulated.

If further required under the Master Agreement, Customer's pre-contracting process or Customer's written instructions, the Provider's suppliers should be certified and attested to confirm compliance the EU-US Data Privacy Framework[8] administered by the US Department of Commerce (if established in the USA) and/or with SOC 2 standards, by independent auditors. Service Organization Controls (SOC) reports must demonstrate its commitment to securing Customer's Personal Data.

[8] Including the equivalent UK-US data privacy adequacy framework ("**Data Bridge**")