Data Processing Addendum

This Data Processing Addendum ("DPA") applies solely to the Processing of Personal Data subject to Data Protection Laws (each as defined below) by Chainyard Supplier Management Inc. (the "Company") on your ("Customer") behalf in connection with the Company's provision of its software-as-a-service, blockchain-based supplier information management system that enables verified information exchange and messaging between third party suppliers and buyers/purchasers (the "Network"). This DPA is subject to the terms and conditions set forth in the agreement, by and between the Company and Customer, that, by its terms, expressly governs Customer's use of the Network (collectively, the "Agreements"). Capitalized terms used and not defined herein have the meanings given to them in the General Data Protection Regulation 2016/679 ("GDPR") or the Agreements, as applicable. In the event of conflict between the DPA and the data processing provisions of the Agreements, the provisions of this DPA shall prevail solely with respect to the Processing of Personal Data.

1. Processing

1.1. Customer: (a) is the sole Controller of Customer Personal Data; or (b) has been instructed by and obtained the authorization of the relevant Controller(s) to agree to the Processing of Customer Personal Data by the Company as set out in this DPA. Customer appoints the Company as Processor to Process Customer Personal Data. If there are other Controllers, Customer will identify and inform the Company of any such other Controllers prior to providing their Personal Data.

1.2. An overview of the categories of Data Subjects, types of Customer Personal Data, special categories of Personal Data and the processing activities is set out in Schedule A attached hereto. The duration of the Processing corresponds to the duration of the term set forth in the Agreements.

1.3. The Company will Process Customer Personal Data according to Customer's written instructions, which Customer agrees, includes instructions inherent in the Company's provision of the Network under the Agreements. The scope of Customer's instructions for the Processing of Customer Personal Data is defined by the Agreements and this DPA. Customer may provide further instructions that are required by applicable law ("Additional Instructions"). If the Company believes an Additional Instruction violates GDPR or other applicable data protection regulations, the Company will inform Customer without undue delay and may suspend Customer's access to the Network until Customer modifies or confirms the lawfulness of the Additional Instruction in writing. If the Company notifies Customer that an Additional Instruction is not feasible or Customer notifies the Company that it does not accept the quote for the Additional Instruction prepared in accordance with Section 10.2 below, the parties agree to work together in good faith to find a reasonable alternative. If the Company notifies Customer that neither the Additional Instruction nor an alternative is feasible, Customer may terminate the affected service by providing the Company with a written notice within one (1) month after notification. The Company will refund a prorated portion of any prepaid charges for the period after such termination date.

1.4. Customer shall serve as a single point of contact for the Company. As other Controllers may have certain direct rights against the Company, Customer undertakes to exercise all such rights on their behalf and to obtain all necessary permissions from the other Controllers. The Company shall be discharged of its obligation to inform or notify another Controller when the Company has provided such information or notice to Customer. Similarly, the Company will serve as a single point of contact for Customer with respect to its obligations as a Processor under this DPA.

1.5. The Company will comply with GDPR and/or any other data protection laws published here (collectively, "Data Protection Laws") in respect of the Network applicable to Processors. The Company is not responsible for determining the requirements of laws applicable to Customer's business or that the Company's provision of the Network meets the requirements of such laws. As between the parties, Customer is responsible for the lawfulness of the Processing of the Customer Personal Data. Customer will not use the Network in conjunction with Personal Data to the extent that doing so would violate applicable Data Protection Laws.

2. Technical and Organizational Measures

2.1. The Company will implement and maintain technical and organizational measures ("TOMs") intended to ensure a level of security appropriate to the risk for the Company's scope of responsibility, which may include: (a) measures to ensure that the Personal Data can be accessed only by authorized personnel for the purposes; (b) the pseudonymization and encryption of Customer Personal Data; (c) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; (d) the ability to restore the availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident; (e) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing of Customer Personal Data; and (f) measures to identify vulnerabilities with regard to the Processing of Customer Personal Data in systems used to provide the Network. TOMs are subject to technical progress and further development. Accordingly, the Company reserves the right to modify the TOMs provided that the functionality and security of the Network are not degraded.

2.2. Customer confirms that the TOMs provide an appropriate level of protection for the Customer Personal Data taking into account the risks associated with the Processing of Customer Personal Data.

3. Data Subject Rights and Requests

3.1. To the extent permitted by law, the Company will inform Customer of requests from Data Subjects exercising their Data Subject rights (e.g. rectification, deletion and blocking of data) addressed directly to the Company regarding Customer Personal Data. Customer shall be responsible for responding to such requests of Data Subjects. The Company will reasonably assist Customer in responding such Data Subject requests in accordance with Section 10.2 below.

3.2. If a Data Subject brings a claim directly against the Company for a violation of its Data Subject rights, Customer will indemnify the Company for any cost, charge, damages, expenses or loss arising from such a claim, to the extent that the Company has notified Customer about the claim

and given Customer the opportunity to cooperate with the Company in the defense and settlement of the claim. Subject to the terms of the Agreements, Customer may claim from the Company amounts paid to a Data Subject for a violation of their Data Subject rights caused by the Company's breach of its obligations under the Data Protection Laws.

4. Third Party Requests and Confidentiality

4.1. The Company will not disclose Customer Personal Data to any third party, unless authorized by Customer, required by law, or otherwise permitted under the Agreements. If a government or Supervisory Authority demands access to Customer Personal Data, the Company will notify Customer prior to disclosure, unless prohibited by law.

4.2. The Company requires all its personnel authorized to Process Customer Personal Data to commit to confidentiality and not Process such Customer Personal Data for any other purposes, except on instructions from Customer or as required by applicable law.

5. Audit

5.1. The Company shall allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer, of the Company's Processing of Customer Personal Data in accordance with the following procedures:

a. Upon Customer's written request, the Company will provide Customer or its mandated auditor with the most recent certifications and/or summary audit report(s), which the Company has procured to regularly test, assess and evaluate the effectiveness of the TOMs.

b. The Company will reasonably cooperate with Customer by providing available additional information concerning the TOMs, to help Customer better understand such TOMs.

c. If further information is needed by Customer to comply with its own or other Controllers' audit obligations, or a competent Supervisory Authority's request, Customer will inform the Company in writing in order to enable the Company to provide such information or to grant Customer access to it.

d. To the extent it is not possible to otherwise satisfy an audit obligation mandated by applicable law, only legally mandated entities (such as a governmental regulatory agency having oversight of Customer's operations), Customer or its mandated auditor may conduct an onsite visit of the facilities used to provide the Network, to the extent under the Company's control, during normal business hours and only in a manner that causes minimal disruption to the Company's business, subject to coordinating the timing of such visit to reduce any risk to the Company's other customers and to Customer' or its auditor's execution of the Company's onsite confidentiality and security statements/policies.

5.2. Each party will bear its own costs in respect of Section 5.1(a) and Section 5.1(b). Any further assistance will be provided in accordance with Section 10.2 below.

6. Return or Deletion of Customer Personal Data

6.1. Subject to the term and conditions set forth in the Agreements, upon termination or expiration of the Agreements, the Company will either delete or return Customer Personal Data in its possession, unless otherwise required by applicable law.

7. Subprocessors

7.1 Customer authorizes the Company to engage subcontractors to Process Customer Personal Data ("Subprocessors"). Customer agrees the Company may continue to use those Subprocessors already engaged by the Company as of the date of this DPA applies to Customer. The Company will notify Customer in advance of any changes to Subprocessors. Within 30 days after the Company's notification of the intended change, Customer can object to the addition of a Subprocessor on the basis that such addition would cause Customer to violate applicable legal requirements. Customer's objection shall be in writing and include Customer's specific reasons for its objection and options to mitigate, if any. If Customer does not object within such period, the respective Subprocessor may be commissioned to Process Customer Personal Data. The Company shall impose substantially similar data protection obligations as set out in this DPA on any approved Subprocessor prior to the Subprocessor Processing any Customer Personal Data.

7.2. If Customer legitimately objects to the addition of a Subprocessor and the Company cannot reasonably accommodate Customer's objection, the Company will notify Customer. Customer may terminate the affected services by providing the Company with a written notice within one (1) month of the Company's notice. The Company will refund a prorated portion of any pre-paid charges for the period after such termination date.

8. Transborder Data Processing

8.1. In the event of a transfer of Customer Personal Data to a country that does not provide an adequate level of protection pursuant to one or more of the applicable Data Protection Laws, the parties shall cooperate in good faith in a manner designed to comply with such applicable Data Protection Laws, as set out in this Section 8. If Customer believes in good faith the measures set out below are not sufficient to satisfy such Data Protection Laws, Customer shall notify the Company thereof and the parties shall work together in good faith to find a reasonable alternative.

8.2. By agreeing to the Agreements, Customer is entering into the contractual clauses set out here pursuant to the European Commission's decision 2021/914 of June 4, 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 ("EU Standard Contractual Clauses"), and any additional safeguards to the EU Standard Contractual Clauses posted here, with: (i) Subprocessors established outside either the European Economic Area or countries considered by the European Commission to have adequate protection; and (ii) the Company. The Company agrees to reasonably cooperate with and provide assistance to Customer, at Customer's sole cost, with respect to any transfer impact assessment required by Data Protection Laws, in connection with any such transfer of personal data.

8.3. If Customer notifies the Company in writing about another Controller and the Company does not object within thirty (30) days after Customer's notification, Customer agrees on behalf of

such other Controller(s), or if unable to agree, will procure agreement of such Controller(s), to be additional data exporter(s) of the EU Standard Contractual Clauses concluded between the Company and Customer. Customer agrees and, if applicable, procures the agreement of other Controllers that the EU Standard Contractual Clauses, including any claims arising from them, are subject to the terms set forth in the Agreements, including the exclusions and limitations of liability. In case of conflict, the EU Standard Contractual Clauses shall prevail.

9. Personal Data Breach

9.1. The Company will notify Customer without undue delay after becoming aware of a Personal Data Breach with respect to the Customer Personal Data. The Company will promptly investigate the Personal Data Breach if it occurred on the Company infrastructure or in another area for which the Company is responsible, and will assist Customer as set out in Section 10 below.

10. Assistance

10.1. The Company will assist Customer by technical and organizational measures, insofar as possible, for the fulfillment of Customer's obligation to comply with the rights of Data Subjects and in ensuring compliance with Customer's obligations relating to the security of Processing, the notification of a Personal Data Breach and the data protection impact assessment, taking into account the information available to the Company.

10.2. Customer will make a written request for any assistance referred to in this DPA. The Company will charge Customer no more than a reasonable charge to perform such assistance or Additional Instructions, such charge to be set forth in a quote and agreed in writing by the parties.

11. Representative in the European Union

11.1 The Company, not being established in a member nation of the European Union, appoints the following individual to be its representative in the European Union in accordance with Article 27 of the GDPR:

Name: Michelle Armstrong
Email Address: michelle.armstrong@itpeoplecorp.com

Phone #: +447889655603

Schedule A

DETAILS OF PROCESSING

Subject matter and duration of the Processing of Personal Data:

The subject matter and duration of the Processing of Personal Data are set out in the Agreements and this DPA.

Nature and Purpose of the Processing of Personal Data:

The Company will process Personal Data for the sole purpose of operating and providing the Network.

Types of Personal Data to be Processed:

First and last name
Business role and/or title
Contact information (company, email, phone, and physical business address)
Localization data (GPS coordinates of business location, as communicated via online mapping)

The Categories of Data Subjects to whom the Personal Data relates:

Employees and agents of network users.

The Obligations and Rights of the Controller:

The obligations and rights of the Controller are set out in the Agreements and this DPA.