Visa Supplier Privacy and Security Terms

These Visa Supplier Privacy and Security Terms ("**P&S Terms**") are entered into by and between Visa U.S.A., Inc. and its Affiliates ("**Visa**"), and the Supplier and its Affiliates identified in the Agreement and/or on the face of the purchase order ("**Supplier**"). These P&S Terms are effective as of the effective date of the Agreement (the "**Effective Date**"). Visa and Supplier may be referred to individually as a "**Party**" or collectively as the "**Parties**."

These P&S Terms are incorporated into and governed by the terms of the applicable Agreement entered into by the Parties for Supplier's provision of Products and/or Services to Visa ("**the Agreement**"). All capitalized terms not defined in this agreement will have the meaning defined in the Agreement. These P&S Terms apply when Supplier performs any operation or set of operations ("**Processes**", "**Process**", "**Processing**") upon any information that, alone or combined with other information, can be associated with an individual or household ("**Personal Information**"), as defined under applicable Privacy Laws. "**Privacy Laws**" means any applicable law, regulation, rule, or other mandatory legal obligation that regulates the collection, use, disclosure, or processing of Personal Information or relates to data protection, data security, or Security Event notification obligations. Supplier will ensure its Sub-processors (as defined in Privacy Laws) comply with these P&S Terms as if they were the Supplier. In the event of a conflict between these P&S Terms, including any attachments, and the Agreement, these P&S Terms will control, but only to the extent that Supplier Processes Personal Information.

Visa and Supplier agree to the following terms:

1. Supplier will only Process Personal Information as permitted by the terms of the Agreement and will comply with all Privacy Laws applicable to it and promptly notify Visa of any circumstances that may prevent it from complying with any Privacy Law.

2. The Parties hereby acknowledge and agree that depending on applicable Privacy Laws, Visa is the Controller or Business and Supplier is acting on behalf of Visa as the Processor or Service Provider (as defined by applicable Privacy Laws) with respect to the Personal Information, except where Visa acts as a Processor of Personal Information, in which case Supplier is a Sub-processor. Supplier will provide reasonable and timely assistance to Visa to ensure ongoing compliance with Privacy Laws.

3. If Supplier's access to, or Processing of, the Personal Information incudes any "personal data," as defined by and subject to the EU General Data Protection Regulation (Regulation (EU) 2016/679, GDPR) or the Privacy Laws of Switzerland or the U.K., then the contractual terms required by such Privacy Laws, including (as applicable) Article 28 of GDPR are hereby incorporated into these terms based on standard contractual clauses between Controllers and Processors under Article 28 (7) of Regulation (EU) 2016/679 and Article 29 (7) of Regulation (EU) 2018/1725 issued by the European Commission on 4 June 2021 (or subsequent versions) ("**Controller to Processor Clauses**") In the event of a conflict between the Controller to Processor Clauses and the P&S Terms, the P&S Terms will prevail. The Additional Protections for European Personal Data set out at: https://usa.review.visa.com/partner-with-us/info-for-partners/info-for-suppliers.html#3 will apply to transfers of European personal data subject to the GDPR or UK GDPR, as applicable. Furthermore, when additional Privacy Laws, including those of Argentina, Brazil, or China, or any applicable jurisdictions, require further protections, any such protections are hereby incorporated into these terms and apply to Personal Information subject to such protections. Supplier will not permit any of its own third-party Sub-processors to access the Personal Information other than included in Annex 2 without Visa's prior written consent.

4. If Supplier Processes Personal Information as a Processor, Service Provider, or Contractor as defined under the California Consumer Privacy Act ("**CCPA**") or similar state laws ("**U.S. State Privacy Laws**"), then the required contract terms, including those in the CCPA and Section 7051 of the CCPA regulations, are incorporated into this Agreement. Supplier certifies it understands and will comply with these restrictions.

5. Supplier will promptly notify Visa of any data subject requests by sending an email to privacy@visa.com. Unless otherwise agreed (such as for handling of requests contemplated by the Agreement), Visa or its Affiliates will handle data subject requests, and Supplier will not disclose any Personal Information in response to any such requests, except to the extent Supplier is required to do so under applicable law. Supplier will reasonably assist Visa with data subject requests as may be required to comply with applicable Privacy Laws.

6. Supplier will establish and implement a written information security program that is consistent with generally accepted industry standards, such as the Cybersecurity Framework issued by the National Institute of Standards & Technology and ISO 270002 to safeguard against the unauthorized disclosure, destruction, loss, or alteration of Personal Information. At a minimum, the written information security program will include: (i) appropriate assessments of cybersecurity risks to Supplier; (ii) an inventory of information systems that contain Personal Information or are otherwise critical to achieving business purposes; (iii) appropriate, risk-informed identity and access management, implementing the principles of least privilege and need-to-know; (iv) encryption of data at rest and in transit, using commercially reasonable encryption; (v) a secure software development lifecycle program for any in-house developed applications that Process, store, or transmit Personal Information; (vi) multi-factor authentication for

access to any information system containing Personal Information except where a reasonably equivalent or more secure access control has been approved in accordance with Supplier's policies; (vii) secure disposal of Personal Information when no longer required for business operations; (viii) procedures for change management; (ix) network security monitoring and logging to detect unauthorized access to, use of, or tampering with Personal Information; (x) regular vulnerability assessments and required remediation timelines for identified vulnerabilities; (xi) deployment of up-to-date, commercially reasonably anti-virus software or similar anti-malware applications; and (xii) periodic training for Supplier's personnel on Supplier's information security program and policy requirements. Supplier represents and warrants that it is not beneficially owned or controlled by a "country of concern" under the implementation regulations of Executive Order 14117 and is complying with such Executive Order.

7. Supplier will promptly investigate all allegations of unauthorized access to, use, destruction, alteration, or disclosure of Personal Information. Supplier will notify Visa of any Security Event in writing without undue delay, but no later than twenty-four (24) hours after determining a Security Event has occurred. This notification must be made via email to vsirt@visa.com. Supplier will reasonably cooperate with Visa in response to a Security Event and provide Visa with all information about the Security Event reasonably needed by Visa to assess its incident response obligations, determine the cause of the Security Event, prevent its recurrence, answer regulatory inquiries, and comply with applicable Privacy Laws. Supplier will not make any statement to other external parties (other than authorized incident response vendors or external legal counsel) concerning a Security Event if the statement identifies Visa, except as required by law or with Visa's written permission. A "**Security Event**" means any occurrence resulting in the actual unauthorized or accidental access to, use, destruction, alteration, disclosure, or inaccessibility of Personal Information, including a "personal data breach" (as defined in the GDPR), a "breach of the security of a system" (as defined in US Privacy Laws), or similar term (as defined in any other applicable Privacy Law).

8. If Supplier's personnel are provided Visa corporate mobile devices (e.g., laptops, phones) to perform services for Visa, Supplier will ensure that such personnel immediately return those assets to Visa (i) upon termination of that individual's employment with Supplier, (ii) if the individual ceases to support Visa services, or (iii) if the Supplier ceases to perform services for Visa. If current or former personnel of Supplier refuse to return the Visa information assets provided, then Supplier will reasonably cooperate with Visa to take all necessary measures to ensure those assets are returned and Visa's Confidential Information and Personal Information are protected from unauthorized disclosure, destruction, or alteration.

9. Suppler will comply with all artificial intelligence laws and regulations and will not use any Personal Information to train any of Supplier artificial intelligence systems or models without the express written consent of Visa.

10. When Supplier ceases to perform services for Visa (and at any other time, upon request), Supplier will purge, delete and destroy the Personal Information.