Data Protection Addendum

1. SCOPE, ORDER OF PRECEDENCE, AND TERM

1.1. This Data Protection Addendum (this "**DPA**") is part of the agreement(s) (the "**Agreement**") between POSaBIT, Inc., a Washington corporation with a business address at 11915 124th Ave NE, Kirkland, Washington 98034 ("**POSaBIT**"), and the signatory to the Agreement ("**Customer**"), as agreed pursuant to the terms of such Agreement. This DPA sets forth the obligations of the Parties with respect to the Processing of Personal Data.

1.2. The effective date of the DPA is the date of the Agreement.

1.3. This DPA applies only with respect to the Personal Data the Parties Process in connection with the activities contemplated by the Agreement.

1.4. In the event of a conflict between this DPA and the Agreement, the DPA will control to the extent necessary to resolve the conflict. In the event the Parties use an International Data Transfer Mechanism and there is a conflict between the obligations in that International Data Transfer Mechanism and this DPA, the International Data Transfer Mechanism will control except as specified in this DPA.

1.5. The term of this DPA is coterminous with the Agreement, except for obligations that survive past termination as specified below.

2. DEFINITIONS

The following terms have the meanings set forth below. All capitalized terms not defined in this DPA will have the meanings set forth in the Agreement.

2.1. "**Controller**" means the entity that determines the purposes and means of the Processing of Personal Data.

2.2. "**Data Protection Law**" means all data protection and privacy laws applicable to the processing of Personal Data under the Agreement.

2.3. "**Data Subject**" means an identified or identifiable natural person.

2.4. "**De-identified Data**" means a data set that does not contain any Personal Data. Aggregated data is De-identified Data. To "**De-identify**" means to create De-identified Data from Personal Data.

2.5. "**Personal Data**" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a Data Subject. Personal Data includes equivalent terms in other Data Protection Law, such as the CCPA-defined term "Personal Information," as context requires.

2.6. "**Personal Data Breach**" means a confirmed breach of security that caused an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of,

or access to Personal Data, or an event that qualifies as a reportable data breach under applicable Data Protection Law.

2.7. "**Process**" or "**Processing**" means any operation or set of operations that a Party performs on Personal Data, including collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

2.8. "**Processor**" means an entity that processes Personal Data on behalf of another entity.

2.9. "**Sell**" has the meaning assigned to it in the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq*., and any successor law.

2.10. "**Sensitive Data**" means the following types and categories of data: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic data; biometric data; data concerning health, including protected health information governed by the Health Insurance Portability and Accountability Act; data concerning a natural person's sex life or sexual orientation; government identification numbers (e.g., SSNs, driver's license); payment card information; nonpublic personal information governed by the Gramm Leach Bliley Act; an unencrypted identifier in combination with a password or other access code that would permit access to a data subject's account; and precise geolocation.

2.11. "**Services**" has the meaning assigned to it in the Agreement. "**Activities**" means the same thing as Services.

2.12. "**Subprocessor**" means a Processor engaged by a Party who is acting as a Processor.

3. SECURITY AND CONFIDENTIALITY

3.1. Security Controls. POSaBIT will maintain a written information security policy that defines security controls that are based on its assessment of risk to Personal Data that it Processes and its information systems. POSaBIT's security controls are described in Schedule 2.

3.2. Confidentiality. Without limiting POSaBIT's confidentiality obligations in the Agreement, POSaBIT will ensure that its employees, independent contractors, and agents are subject to an obligation to keep Personal Data confidential.

4. DESCRIPTION OF THE PARTIES' PERSONAL DATA PROCESSING SERVICES AND STATUSES OF THE PARTIES

4.1. Schedule 1 describes the purposes of the Parties' Processing, the types or categories of Personal Data involved in the Processing, and the categories of Data Subjects affected by the Processing.

4.2. Schedule 1 lists the Parties' statuses under relevant Data Protection Law.

5. INTERNATIONAL DATA TRANSFER

5.1. Some jurisdictions require that an entity transferring Personal Data to, or accessing Personal Data from, a foreign jurisdiction take extra measures to ensure that the Personal Data has special protections (an "**International Data Transfer Mechanism**"). The Parties will comply with any International Data Transfer Mechanism that may be required by applicable Data Protection Law. Before Customer transfers to POSaBIT, or permits POSaBIT to access, Personal Data originating from a jurisdiction that requires an International Data Transfer Mechanism, Customer will notify POSaBIT of the relevant requirement and the Parties will work together in good faith to fulfill the requirements of that International Data Transfer Mechanism.

6. DATA PROTECTION GENERALLY

6.1. Compliance. The Parties will comply with their respective obligations under Data Protection Law and their privacy notices. The Parties will notify each other if they are no longer able to comply with applicable Data Protection Law.

6.2. Lawful Basis of Processing. If Customer is required by Data Protection Law to have a lawful basis of Processing Personal Data, such as consent, Customer represents and warrants that it collects Personal Data consistent with such requirement.

6.3. Cooperation.

6.3.1. Governmental and Investigatory Requests. If either Party receives any type of request or inquiry from a governmental, legislative, judicial, law enforcement, or regulatory authority (e.g. the Federal Trade Commission, the Attorney General of a U.S. state, or a European data protection authority), or faces an actual or potential claim, inquiry, or complaint in connection with the Parties' Processing of Personal Data (collectively, an "**Inquiry**"), the receiving Party with notify the other Party without undue delay unless such notification is prohibited by applicable law. If requested by the receiving Party, the other Party will provide the receiving Party with information relevant to the Inquiry to enable the receiving Party to respond to the Inquiry.

6.3.2. Other Requirements of Data Protection Law. Upon request, the Parties will provide relevant information to each other to fulfill their respective obligations (if any) to conduct data protection impact assessments or prior consultations with data protection authorities.

6.4. De-identified, Anonymized, or Aggregated Data. The Parties may create De-identified Data from Personal Data and Process the De-identified Data for any purpose.

7. POSABIT'S OBLIGATIONS AS A PROCESSOR

7.1. The obligations set forth in this Section 7 apply only in connection with POSaBIT's Processing of Personal Data of Customers in its capacity as Customer's Processor in connection with the Services; these obligations do not apply to POSaBIT in its capacity as a Controller.

7.2. Scope of Processing.

7.2.1. POSaBIT will Process Personal Data solely in connection with the Services, to carry out its obligations under the Agreement, and to carry out Customer's documented instructions. POSaBIT will not Process Personal Data received from Customer in connection with the Agreement for any other purpose, unless required by applicable law, and will not Sell Personal Data received from Customer in connection with the Agreement.

7.2.2. Notwithstanding anything to the contrary, the Parties agree that POSaBIT may, and Customer instructs POSaBIT to, Process Personal Data for internal operations that support the Services, including to detect data security incidents; protect against fraudulent or illegal activity; ensure safety; debug, troubleshoot, or repair products and services; provide customer service; maintain or service accounts; undertake internal research for technological development; and build or improve the quality of POSaBIT's products and services.

7.2.3. Processing any Personal Data received from Customer in connection with the Agreement outside the scope of the Agreement will require prior written agreement between POSaBIT and Customer by way of written amendment to the Agreement.

7.2.4. POSaBIT will notify Customer if it believes that it cannot follow Customer's instructions or fulfil its obligations under the Agreement because of a legal obligation to which POSaBIT is subject, unless POSaBIT is prohibited by law from making such notification.

7.3. Data Subjects' Requests to Exercise Rights. POSaBIT will promptly inform Customer if POSaBIT receives a request from a Data Subject to exercise their rights with respect to their Personal Data under applicable Data Protection Law. Customer will be responsible for responding to such requests. POSaBIT will not respond to such Data Subjects except to acknowledge their requests. POSaBIT will provide Customer with commercially reasonable assistance, upon request, to help Customer to respond to a Data Subject's request.

7.4. POSaBIT's Subprocessors. POSaBIT and its Subprocessors will enter into agreements that require the Subprocessor to meet obligations that are no less protective of Personal Data than this DPA.

7.5. Personal Data Breach. POSaBIT will notify Customer without undue delay of a Personal Data Breach affecting Personal Data POSaBIT Processes in connection with the Services. Upon request, POSaBIT will provide information to Customer about the Personal Data Breach to the extent necessary for Customer to fulfill any obligations it has to investigate or notify authorities, except that POSaBIT reserves the right to redact information that is confidential or competitively sensitive. Notifications will be delivered to the contact addresses listed in the Agreement. Customer agrees that email notification of a Personal Data Breach is sufficient. Customer agrees that it will notify POSaBIT if it changes its contact information. Customer agrees that POSaBIT may not notify Customer of security-related events that do not result in a Personal Data Breach.

7.6. Deletion and Return of Personal Data. At the expiration or termination of the Agreement and upon written request by Customer to POSaBIT, POSaBIT will, without undue delay, (1) return all Personal Data (including copies thereof) to Customer and/or (ii) destroy all Personal Data (including copies thereof), except to the extent reasonably necessary to meet POSaBIT's legal compliance obligations or pursuant to POSaBIT's records management and backup program and policies (including retention reasonable required for the enablement of internal and external audits) or the Parties otherwise expressly agree in writing. For any Personal Data that POSaBIT retains after expiration or termination of the Agreement (for example, because POSaBIT is legally required to retain the information), POSaBIT will continue to comply with the data security and privacy provisions of this DPA and POSaBIT will De-identify such Personal Data (if any) to the extent feasible.

7.7. Audits.

7.7.1. Scope. The terms of this Section 7.7 apply notwithstanding anything to the contrary. Customer agrees that POSaBIT's obligations under this Section 7.7 are limited to the Personal Data POSaBIT Processes in connection with the Services.

7.7.2. Request. Upon written request that includes a statement of reasons for the request, POSaBIT will make available to Customer applicable documentation that is responsive to Customer's request, including third-party audit reports or certifications to the extent they are available. To the extent that such audit reports or certifications do not satisfy Customer's request, POSaBIT will provide Customer or Customer's designated third party (which Customer agrees may not be a competitor to POSaBIT) with the information and access to facilities necessary to demonstrate compliance with Data Protection Law.

7.7.3. Access to Facilities. If Customer requires access to POSaBIT's facilities (the "**Inspection**"), Customer will provide POSaBIT with written notice at least 60 days in advance. Such written notice will specify the things, people, places, or documents to be made available. Such written notice, and anything produced in response to it (including any derivative work product such as notes of interviews), will be considered confidential information and will remain confidential information in perpetuity or the longest time allowable by applicable law after termination of the Agreement. Such materials and derivative work product produced in response to the Inspection will not be disclosed to anyone without the prior written permission of POSaBIT unless such disclosure is required by applicable law. If disclosure is required by applicable law, Customer will give POSaBIT prompt written notice of that requirement and an opportunity to obtain a protective order to prohibit or restrict such disclosure except to the extent such notice is prohibited by applicable law or order of a court or governmental agency. Customer agrees to negotiate in good faith with POSaBIT before seeking to exercise such audit or on-site inspection right more frequently than once per twelve (12) month period. Customer will make every effort to cooperate with POSaBIT to schedule the Inspection at a time that is convenient to POSaBIT. Customer agrees that if it uses a third party to conduct the Inspection, the third party will sign a non-disclosure agreement. Customer agrees that the Inspection will only concern POSaBIT's architecture, systems, policies, records of processing, data protection impact assessments, and procedures relevant to its obligations as set forth in the Agreement.

Customer agrees that POSaBIT shall be allowed to protect or redact the names and identifying or proprietary information of other POSaBIT customers during the Inspection.

7.8. Additional Terms. As a condition to Customer's access and use of any documentation, reports, materials or facilities under this Section 7 (either directly or through a third party), POSaBIT may require Customer to agree to certain terms and conditions requested by POSaBIT, including additional confidentiality and non-disclosure requirements, covenants to comply with POSaBIT's policies, and the requirement to implement and comply with a mutually agreed upon inspection plan.

Schedule 1: Description of Personal Data Processing

Processing Activity	Status of the Parties	Categories of Personal Data Processed	Categories of Sensitive Data Processed
POSaBIT processes Customer information to facilitate the Services, e.g., offering a SaaS-based point-of-sale solution, offering payment processing, or enabling Customers to use third-party APIs to facilitate inventory management, loyalty programs, bookkeeping, analytics, and other services.	Customer is a Controller. POSaBIT is a Processor.	The following are representative categories of data that may include Personal Data: • Customer IDs • Customer phone numbers • Transaction information associated with payment card information (see above), Customer IDs, or other Customer Personal Data • Customer payment card information (note: POSaBIT does not process or have access to the full payment card number (PAN)) • Driver's license information (if the Customer is a member of Customer's loyalty program) • Customer loyalty and reward program information • Limited medical information: medical #, medical expiration, caregiver ID, caregiver expiration • Product and sales information	Payment card information
The Parties Process Personal Data of their employees to, e.g., administer and conduct the Services; manage invoices; manage the Agreement and resolve any disputes relating to it; respond and/or raise general queries; comply with their respective regulatory obligations; and create and administer web-based accounts.	Customer is a Controller. POSaBIT is a Processor.	• Employee name, title, and other contact information • Employee POSaBIT PIN IDs • Device and/or activity Data related to a Customer's employees' clicks, presses, or other interactions with POSaBIT hardware and software	None

Schedule 2: Technical and Organizational Security Measures

POSaBIT has implemented a written information security policy that addresses:

- Roles and responsibilities for managing security controls.
- Employee disciplinary measures.
- Exceptions management.
- Risk assessments.
- Employee training.
- Asset management and encryption.
- Physical and environmental security.
- Access controls.
- Logging and monitoring.
- Incident response.
- Business continuity and disaster recovery.
- Mobile devices and telework.

Furthermore, POSaBIT uses a secure, third-party solution to facilitate transfers of Personal and confidential data to and from its clients. POSaBIT also performs a 3rd party security review annually to review its security procedures and practices.