THE J.M. SMUCKER Co

SECURITY MEASURES

Version: November 2, 2023

In the event that any provisions of this Exhibit are inconsistent or conflict with the terms of the Agreement and/or any Statement of Work, purchase order, insertion order, or other terms between the Parties, the provisions of this Exhibit shall govern. The obligations herein shall survive expiration or termination of the Agreement to the extent that Service Provider has any Smucker Proprietary Data (as hereafter defined) in its possession or control. Capitalized terms not otherwise defined herein shall have the meanings assigned to them in the Agreement.

1. Definitions.

    a. "**Applicable Law**" means all applicable laws, rules, regulations, ordinances, rulings, decisions, regulatory guidance and interpretations, and industry guidelines, all as may be enacted, amended, restated, or replaced from time to time.

    b. "**Personal Data**" means any information that identifies, relates to, describes, is capable of being associated with or identifying, or could reasonably be linked (directly or indirectly) with a particular individual, consumer, household, or device, which includes, without limitation, any inferences drawn about individuals, consumers, households, or devices, or derivatives thereof, and/or any other information that is regulated as "personal data," "personally identifiable information," "personal information," or similar term as otherwise defined under Applicable Law.

    c. "**Processed"** means access, use, maintain, store, collect, modify, adapt, merge, analyze, combine, aggregate, transfer, disseminate, retain, erase, process, and/or disclosed.

    d. "**Smucker Personal Data**" means i) any Personal Data that is collected by or on behalf of, identifies, relates to, describes, is capable of being associated with or identifying, or could reasonably be linked (directly or indirectly) with Smucker, including without limitation, any Personal Data that relates to or could be associated with Smucker's employees, customers, and/or prospects, and/or other end-users of Smucker's products, services, websites, advertisements, or content; and ii) any Personal Data acquired by or obtained by or on behalf of Smucker, or Processed by or on behalf of Smucker, or made available to Service Provider or any third party on behalf of Smucker in connection with, or in relation to, the Agreement, this Exhibit, and/or the provision of any products or services to, or on behalf of, Smucker. Smucker Personal Data includes any aggregated, deidentified or other derivative of other Smucker Personal Data.

    e. "**Smucker Proprietary Data**" means all Smucker Personal Data and all Smucker confidential information, proprietary information, and trade secrets (but excluding trade secrets covered under the Trade Secret Addendum of the Agreement in those instances in which the Trade Secret Addendum applies to such trade secrets).

2. Security. Service Provider represents, warrants, and covenants that it has adopted and implemented, and will maintain and enforce for as long as the Agreement is in effect or as long as Service Provider stores or Processes Smucker Proprietary Data (whichever is later), an information security program appropriate to the nature of the Processing and the Smucker Proprietary Data involved or as otherwise required by Applicable Law that includes administrative, organizational, technical, physical, and other safeguards sufficient to protect Personal Data and Smucker Proprietary Data against accidental, unauthorized or unlawful Processing, destruction, loss, alteration, communication, use, disclosure, and access, and against all other unlawful activities, and that complies with all Applicable Law. Without limiting the generality of the foregoing, Service Provider warrants that it shall at all times comply with or operate in alignment with all security standards and procedures set forth in the Center for Internet Security CIS Controls 8.0 for Implementation Group 3 (or successor version) and shall have in place, at a minimum,

safeguards that provide for and ensure: (a) protection of business facilities, paper files, servers, computing equipment, including without limitation all mobile devices and other equipment with information storage capability, and backup systems containing Personal Data and Smucker Proprietary Data; (b) network, application (including databases) and platform security, including secure network and software design and coding, and controlled software development and promote to production processes; (c) business systems designed to optimize security and proper disposal of Smucker Proprietary Data according to the terms of this Exhibit; (d) secure transmission and storage of Personal Data and Smucker Proprietary Data, including encryption of data in transmission and at rest; (e) authentication and access control mechanisms over Smucker Proprietary Data, media, applications, operating systems and equipment, ensuring that user IDs are unique among users and not shared, and utilizing industry standard password selection and aging procedures and multi-factor authentication; (f) personnel security and integrity, including background checks where consistent with applicable law; (g) annual training to Service Provider's employees on how to comply with the Service Provider's physical, technical, and administrative information security safeguards and confidentiality obligations under Applicable Law; (h) up to date versions of security agent software for systems that house Smucker Proprietary Data, which include malware protection, and use up to date patches and virus definitions; (i) storage limitations such that Smucker Proprietary Data resides only on servers in data centers that comply with industry standard data center security controls, and restrictions to ensure that Smucker Proprietary Data files are not placed on any notebook hard drive or removable media, such as compact disc or flash drives; (j) identification of reasonably foreseeable internal and external risks on a regular basis, and assessments of the sufficiency of existing safeguards in relation to such risks; (k) regular monitoring and testing of the design and operating effectiveness of key controls, systems, and procedures, and prompt remediation of ineffective controls; (l) regular testing of backup and incident response recovery processes; (m) prompt implementation of any adjustments to the information security program and Service Provider's safeguards in light of business changes or new threats, technologies, and circumstances; (n) role-based access control lists maintained and enforced with access to assets and information limited to individuals on a need-to-know basis; (o) standardized logging and monitoring of all cybersecurity events and activities; and (p) multilayered boundary defenses (e.g., firewalls, web proxies, DMZ perimeter networks, and other network based tools). Service Provider shall separate and segregate Smucker Proprietary Data from its other clients' data and ensure strong authentication and authorization controls are in place to gain access to Smucker Proprietary Data. For all systems that store or transmit Smucker Proprietary Data, Service Provider shall run internal and external network vulnerability scans at least quarterly and after any material change in the network configuration; Service Provider shall promptly remediate vulnerabilities identified in such scans. Smucker Proprietary Data shall not be Processed or stored in a cloud or outsourced environment unless preapproved by Smucker in writing and there is transport encryption for communications with and among cloud or outsourced elements.

3. Smucker Systems. In the event Service Provider accesses any Smucker system, infrastructure, software, hardware, property, computer, device, information network, or equipment (collectively, "**Smucker Systems**"), Service Provider shall: i) connect only in the manner and through the means authorized by Smucker and in accordance with any policies, guidelines, or restrictions provided by or on behalf of Smucker; ii) not connect, access, or use (nor attempt to connect, access, or use) any Smucker System without the prior authorization of Service Provider; iii) not use personal or shared accounts; iv) not attempt to gain unauthorized access to any Smucker System or other user's account; v) not, nor attempt to, use any Smucker System in any way that is illegal; is abusive; is harmful to or interferes with Smucker's other networks or systems or the networks or systems of any other entity; infringes, misappropriates, or otherwise violates the privacy, proprietary, or other rights of any party; or creates a security risk or vulnerability; vi) be responsible for all Smucker equipment issued or in Service Provider's possession or control; and vii) return any Smucker equipment when no longer required to complete the services under the Agreement, if the Agreement is terminated, or immediately upon Smucker's request. Notwithstanding anything to the contrary contained herein, Service Provider shall be deemed to be in material breach of this Exhibit in the event that the acts or omissions of Service Provider or any of Service Provider's Representatives cause, result in, or contribute to any damage to, unauthorized or accidental access to, unauthorized Processing of, loss of, unauthorized disclosure, acquisition, use, reproduction, destruction, or deletion of, vulnerability to, or misuse of any Smucker System, database, data, or materials.

4. Encryption. Service Provider shall ensure that (a) any Smucker Proprietary Data transmitted over a network, whether via email, file transfer protocol, or other means of electronic exchange, (b) any Smucker Proprietary Data stored on a portable device, including but not limited to a laptop computer, and (c) any Smucker Proprietary Data stored in backup or replicated storage areas shall be encrypted using a

cryptographic algorithm employing a key length of at least 256 bits. For avoidance of doubt, as indicated above in Section 2 of this Exhibit (and, in Section 1.3(c) of Exhibit **C** of the Agreement, where applicable), Smucker's policy prohibits Service Provider from placing or storing any Smucker Proprietary Data on any notebook hard drive or removable media, such as compact disc, floppy disc, or USB flash drives.

5. PCI Compliance. To the extent applicable to the services provided under the Agreement, Service Provider acknowledges that it is responsible for the security of the credit, debit or other cardholder payment information it Processes, and hereby represents and warrants that it will comply with the most current Payment Card Industry ("**PCI**") standards in connection with the Processing of such data, including, but not limited to: (a) creating and maintaining a secure network to protect cardholder data; (b) using all technical and procedural measures reasonably necessary to protect cardholder data it maintains or controls; (c) creating and implementing secure measures to limit access to cardholder data; (d) monitoring access to cardholder data it maintains or controls; and (e) creating and implementing an information security policy that assures employee compliance with the foregoing. To the extent applicable, Service Provider acknowledges that it is responsible for maintaining compliance with the then-current PCI Data Security Standard ("**PCI DSS**") requirements (which requirements are incorporated herein by reference) and monitoring the PCI DSS compliance of all associated third parties Service Provider may provide with access to cardholder data in accordance with the terms of the Agreement.

6. Written Program. Service Provider represents and warrants that it has in place all appropriate written policies containing reasonable and appropriate administrative, physical, organizational and technical safeguards that, at a minimum, meet the applicable requirements in this Exhibit, including: (a) a written program instructing its employees, contractors, agents, and Service Providers how to protect Personal Data and Smucker Proprietary Data, and (b) a written security incident response plan detailing the procedures for managing suspected and actual Data Incidents and assigning personnel roles and responsibilities related to same. Service Provider further represents and warrants that it shall use all necessary steps to protect Personal Data and Smucker Proprietary Data, including conducting on a regular basis assessments of foreseeable internal and external risks to the security, confidentiality and integrity of electronic, paper and other records containing Personal Data and/or Smucker Proprietary Data, and as necessary improving the effectiveness of its safeguards to limiting such risks, including employee training, ensuring ongoing employee compliance with its written program, and the development of measures for detecting and preventing security system failures. Service Provider has identified a specific representative to be in charge of its program and shall ensure that this individual (or a designated alternate) is available to Smucker to respond to any questions and to work with Smucker in the event of any incident or suspected incident involving Smucker Proprietary Data and/or impacting the security, integrity, availability, or confidentiality of Smucker Proprietary Data.

7. Audit and Inspection. Upon Smucker's request, Service Provider will complete Smucker's Third-Party Technical Risk Assessment ("**3PTRA**") and will update its responses to the 3PTRA on the earlier of (i) a change in Service Provider's or its subcontractor's control environment, or (ii) one year from the date of the then current 3PTRA. Smucker reserves the right to conduct (by itself or through a designated, reputable third party) ongoing manual and/or automated reviews, scans, audits, and assessments, including, without limitation, on-site audits and testing of any locations where Smucker Proprietary Data is stored or otherwise processed, to monitor, assess, and ensure Service Provider's compliance with its obligations under Applicable Law and this Exhibit, including compliance with PCI DSS requirements where applicable. Service Provider shall otherwise cooperate with Smucker in Smucker's efforts to monitor Service Provider's compliance. On an annual basis, Service Provider will provide a current SSAE18 SOC II Type II audit, or other audit acceptable to Smucker in its sole discretion, of Service Provider's internal controls. Service Provider will promptly, at its sole expense, remediate any material deficiencies identified in any audit and provide documentation of its remediation of such deficiencies to Smucker. In the event Service Provider makes any material changes to the security safeguards applicable to the locations, servers, systems, or databases where Smucker Proprietary Data is stored or otherwise Processed, Service Provider shall certify in writing that the changes will not in any way diminish or weaken the security or integrity of the Smucker Proprietary Data stored or otherwise Processed therein. Service Provider acknowledges and agrees that a threatened or actual breach of this Exhibit will result in irreparable harm for which monetary damages may not provide a sufficient remedy, and that in addition to all other remedies, Smucker shall be entitled to obtain specific performance and injunctive relief, specifically to protect against a such breach of this Exhibit.