THE J.M. SMUCKER Co

EXHIBIT C
SERVICE PROVIDER ACCESS REQUIREMENTS

Version: May 28, 2025

Service Provider will ensure that Service Provider Personnel (i) are aware of the Service Provider Access Requirements and (ii) strictly adhere to these in the performance of any Services at a Smucker Facility or on the Smucker Network. Reference to Service Provider in this Exhibit will be deemed to include collectively Service Provider and Service Provider Personnel.

1. **INFORMATION TECHNOLOGY AND SECURITY**.

1.1. "**Service Provider Device**" is any device used by Service Provider to access the Smucker Network, including, without limitation, to any personal computer, tablet, or mobile device.

1.2. Service Provider will ensure that in connection with access to, or use of, the Smucker Network by Service Provider, it will:

(a) Strictly limit all access on the Smucker Network to the application, server, or equipment which is required by Service Provider for carrying out the Services under the Agreement;

(b) Install a commercially available anti-virus package installed on any Service Provider Device, configured for real-time virus protection, and to automatically update for pattern or definition files to the latest version and use its best efforts to protect Service Provider's local area network and Service Provider Devices from malware, spyware and viruses;

(c) Install current security patches on any Service Provider Device operating system and applications; and

(d) Install a commercially available encryption package on any Service Provider Devices containing Smucker information, including, without limitation, email, documents, and drawings.

1.3. Service Provider will ensure that in connection with access to, or use of, the Smucker Network by Service Provider, it will <u>not</u>:

(a) Change, install or deploy any software, agents, or other programming components or make unauthorized changes to any component of the Smucker Network without prior written approval from an authorized Smucker employee;

(b) Use hardware device or software application capable of scanning the Smucker Network, computer hardware, system software, desktop, laptop, other computing resource, or business application without prior written consent by an authorized Smucker employee, which written consent must be received prior to each engagement of such scanning event;

(c) Use any public or private, internet, or personal storage service to store Smucker data or information, including, without limitation, Smucker Confidential Information and Personal Data, nor receive, forward, or store email in support of the Services on consumer email services including, without limitation, Yahoo, Google, or Microsoft (e.g. Gmail, Yahoo mail, etc.); and

(d) Smucker will require all Service Provider Personnel needing access to the Smucker Network to enroll in Multi-Factor Authentication.

1.4. Smucker requires that any Service Provider Device be presented to Smucker for Smucker to validate the existence of the anti-virus software, encryption software and operating system patches before connecting to the Smucker Network. Smucker reserves the right to scan Service Provider Devices for Smucker data and viruses and other forms of malware.

1.5. Smucker reserves the right to immediately, and without warning, revoke all access rights and privileges if: (i) the Agreement is terminated or expires or (ii) it is determined that Service Provider or anybody using Service Provider's physical or systems access credentials has violated these rules or has in any other way compromised the confidentially, integrity or availability of any portion of the Smucker Network.

1.6. Access to the Smucker Network is subject to the following additional restrictions and requirements:

(a) By default no access will be granted to any private data on the Smucker Network. If access has been requested and approved, Service Provider must manually map a drive to that data. No automated login script will be supplied.

(b) Remote access tokens (i.e. SecurID) will be provided to Service Provider if required. Smucker may issue software-based tokens to Service Provider if using Smucker owned computer equipment but these tokens may not be used on any non-Smucker owned computer equipment.

(c) The Smucker Corporate Help Desk provides support for remote access requirements. Contact the Help Desk for assistance. Please listen to the system message after business hours for additional contact information.

2. WORK PRACTICES, POLICIES AND PROCEDURES.

2.1. Service Provider represents, warrants and covenants that Service Provider will not assign any Service Provider Personnel under the age of 18 years to any Smucker Facility.

2.2. Service Provider will ensure that Service Provider Personnel strictly comply with Smucker's site rules, workplace policies and procedures, and safety regulations applicable to any Smucker Facility where Service Provider is performing Services. In addition, should any Services be conducted at a Smucker Facility where Smucker products, or any material that will be used in the production of Smucker products ("**Smucker Production Facility**"), are produced or stored, Service Provider will ensure that Service Provider Personnel strictly comply with any Good Manufacturing ("**GMP**") regulations as established by the Food and Drug Administration. All Service Provider Personnel entering a Smucker Production Facility must read and agree to abide by all GMP regulations and site-specific rules and regulations prior to entering any Smucker Production Facility.

2.3. Service Provider Personnel may not use tobacco, intoxicants or any drug or drug-like substance whose sale, use, or possession is unlawful, or any prescribed substance without a prescription ("**Controlled Substance**") on Smucker property. Service Provider will direct its employees not to possess or distribute any Controlled Substance or alcoholic beverage at any Smucker Facility or while Service Provider Personnel are representing Smucker on a third party's premises. Employees not complying with this subsection will be banned from Smucker Facilities.

2.4. Service Provider will ensure that Service Provider Personnel do not carry firearms or any other weapons while at a Smucker Facility, including parking lots.

2.5. Service Provider will ensure that it has completed reasonable preemployment screenings for Service Provider Personnel in compliance with Service Provider's internal policies, practices, and applicable laws and regulations, to ensure that Service Provider Personnel are legally authorized to work in the jurisdiction where the Services are being provided and have the necessary qualifications, skills, education, and training to perform the Services.

3. BUILDING SECURITY

3.1. Service Provider Personnel will be assigned a visitor's badge. The visitor's badge is to be visible while Service Provider Personnel are in the building.

3.2. For extended projects, the Smucker project manager may request that Service Provider Personnel be issued a contractor's identification badge. The badge is the property of Smucker and must be surrendered to the Smucker project manager at the completion of the project or upon the request of an authorized Smucker employee.

(a) The identification badge will provide access to the Service Provider's primary building during normal business hours.

(b) After hours, secured area, and/or multiple building access may be granted on an exception basis, for a limited period of time.

3.3. No external, stairwell or locked doors should be propped open and left unattended.

3.4. Only Service Provider Personnel with a specific need will be permitted in the secure areas of the buildings and the Service Provider Personnel will be accompanied by a Smucker employee in those areas unless specific access has been granted in accordance with Section 3.2(b) above.

3.5. Service Provider acknowledges and agrees that parcels, packages, briefcases, bags, and similar items carried by Service Provider Personnel will be subject to inspection by security representatives of Smucker.

3.6. Service Provider will immediately inform Smucker's site security contact of any credible threat made against anyone at a Smucker Facility and/or against Smucker's property by any Service Provider Personnel.

4. OPERATION OF MOTOR VEHICLES. Unless otherwise mutually agreed in writing, Service Provider Personnel are not permitted to operate any of Smucker's motor vehicles. If such a mutual agreement is reached, Service Provider will select only Service Provider Personnel with a valid driver's license and no DUI, DWI or reckless operation convictions and will cause such employees (i) to use Smucker's motor vehicles only for completion of specific work assignments as designated by Smucker and for no other purpose, (ii) to operate Smucker's motor vehicles in a safe manner at all times, and (iii) to obtain their written acknowledgment that they understand and agree to use of such vehicles as prescribed.