The Campbell's Company Data Security Requirements

1. **Definitions.**

a. "**Client**" shall mean The Campbell's Company entity that is a party to the underlying agreement, including purchase orders, to which these Data Security Requirements are attached (the "Agreement").

b. **"Client data"** means any or all of the following, and all copies thereof, regardless of the form or media in which such items are held: (a) confidential information of Client, including personal information or personal data as defined by applicable data privacy laws and regulations; (b) data and/or information provided or submitted by or on behalf of Client to Vendor regardless of whether considered confidential information; and (c) data and/or information submitted, stored, recorded, processed, created, derived or generated by Vendor as a result of and/or as part of the provision of Services, regardless of whether considered confidential information.

c. "**Personal Information"** means any information that identifies, relates to, describes, is linked to, reasonably capable of being associated with, or could reasonably be linkable, directly or indirectly, with an identified or identifiable individual or household, as well as other information defined as "personal information" or "personal data" under Applicable Data Protection Laws. Personal Information includes "sensitive personal information" or "sensitive data" under Applicable Data Protection Laws.

d. "**Process" or "Processing**" means any operation or set of operations which is performed on Personal Information or on sets of Personal Information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

e. "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of Company by Vendor pursuant to the Agreement.

f. "**Vendor**" shall mean the counterparty to the Agreement, including its affiliates or subsidiaries, or the seller, including its affiliates and subsidiaries, on the relevant purchase order.

g. **"Vendor Personnel"** means any employee, agent, contract employee, independent contractor, subcontractor, or other third party acting on behalf of Vendor that is engaged, in some form, in the Processing of Client data.

h. "**Security Breach"** means an event where Client data has been, or Vendor believes that it has been, acquired, destroyed, modified, used, disclosed, or accessed by any person in an unauthorized manner or for an unauthorized purpose.

2. **Disengagement Services**. Vendor shall provide disengagement services in all circumstances in which the Agreement terminates or expires for up to [60] days after the date of termination or expiration (the "**Disengagement Period**"). Throughout the Disengagement Period, Vendor shall (i) continue to provide the Services pursuant to the terms of this Agreement until notified by Client in writing that the Services are no longer required, (ii) cooperate with Client in effecting the orderly transfer of the Services, and
(iii) perform such additional services as may be requested by Client in accordance with this Section in connection with the transfer of Services to a third party or the assumption of the Services by Client (collectively, the "**Disengagement Services**"). The quality and level of performance during the Disengagement Period shall not be degraded. Vendor shall provide the Disengagement Services at Vendor's rates for such services then in effect immediately prior to such expiration or termination. After the expiration of the Disengagement Period, Vendor shall answer questions from Client regarding the Services on an "as needed" basis at Vendor's then standard commercial billing rates.

3. **Data Ownership**: Vendor acknowledges and agrees that, as between Client and Vendor, Client retains ownership of all right, title and interest to the Client data. Vendor shall not access, share, or otherwise process Client data, except (i) to provide the Services,
(ii) to respond to service or technical problems, or (iii) at Client's request.

4. **Data Retrieval / Portability**: Vendor shall retain all Client data, including all related electronic records, and copies generated in the course of Vendor's ordinary back up procedures, power or control (i) in commercially portable format, (ii) preserving its record functionality and associated metadata, and (iii) in a manner that ensures that all such Client data is accessible in a timely manner, searchable, readable, and retrievable.

5. **Data Retention and Destruction**: Vendor may retain Client data only for the period of time required for Vendor to perform the Services, or such longer period if required by applicable law, the Agreement, pursuant to Client's data retention and destruction policy, or as otherwise requested by Client in writing. Upon termination or expiration of the Agreement for any reason, at any time upon Client's written request, or when retention is no longer permitted by applicable law or policy, Vendor shall promptly return all Client data to Client in a commercially portable format requested by Client. Vendor will never refuse for any reason, including Client's material breach of this Agreement, to provide Client with the Client data in accordance with this paragraph. Client may request that Vendor, for a specified period or indefinitely, until further notice, ceases to destroy any portion, or all, of the Client data for purposes of a legal

hold, by giving Vendor at least a 15-day notice. If so requested, Vendor shall, during the period specified in the foregoing notice (i) refrain from deleting or otherwise destroying the Client data, (ii) retain all Client data in conformance with the retention requirements set forth herein, and (iii) provide all Client data to Client immediately upon its request, at no additional charge. Within a reasonable period of time of receiving the foregoing notice, Vendor shall take all necessary steps to suspend destruction policies and to ensure the preservation of relevant records until written clearance is received from the Client's legal department. Within ninety (90) days of termination of this agreement Client shall provide Vendor with written direction as to the disposition of Client data. Client may request the return of the Client data in Client's specified format or the destruction of the data at no cost to Client. Vendor shall provide a certificate of destruction to Client.

6. **Data Security**: Vendor represents and warrants that it has implemented and will maintain appropriate administrative, technical and physical safeguards that (a) protect against anticipated threats or hazards to the integrity and security of, the unauthorized or accidental destruction, loss, alteration or use of, and the unauthorized access to, Client data, (b) ensure that changes to any Client data are authorized, and are complete, accurate and timely, (c) ensure all Client data accessed in connection with the Services is collected, used, disclosed and retained only as agreed to by Client, and in a manner that complies with all applicable laws and regulations, and (d) meet or exceed the standards and guidelines issued by the Center for Internet Security, the Information Security Management Systems Requirements and ISO-IEC 27000 series, or the standards and guidelines issued by the National Institute for Standards and Technology, as each may be periodically updated or replaced by industry specific privacy or security requirements. Without limiting the foregoing, Vendor further represents and warrants as follows:

   a) Vendor has written comprehensive security policies, procedures and practices that comply with the data security obligations of such laws, regulations, and industry requirements, which include, without limitation, the following safeguards: (i) secure business facilities, data centers, paper files, servers, back-up systems and computing equipment including, but not limited to, all mobile devices and other equipment with information storage capability; (ii) network, device application, database and platform security; (iii) secure transmission, storage and disposal; (iv) deployment of up-to-date security systems, computers and technologies, including malware protection, virus definitions, patches, updates, firewalls, intrusion detection, logging, monitoring and encryption technologies; (v) password protection, authentication and access controls within media, applications, operating systems and equipment; and (vi) encryption of Client data at all times, in transit and at rest.

b) In no event will Client data be stored permanently or temporarily on any mobile devices (including, without limitation, laptops), nor processed in test, development or non-production environments, or comingled with data of other clients of Vendor;

c) Vendor maintains a personnel security and integrity program that includes, but is not limited to, (i) background checks consistent with applicable law and the requirements of this Agreement; (ii) restriction of use and copying of Client data on a "need-to-know" basis; and (iii) data security and privacy training. Vendor shall remove all Client data from any media taken out of service and shall destroy or shall securely and effectively erase such media such that Client data cannot be retrieved, recreated, or reassembled.

d) Vendor agrees to maintain the software patching and malware protection / antivirus software for all equipment that it uses to connect to Client's network, in each case, in accordance with Client's Information Technology Security Standards. Vendor acknowledges that such standards require that all software patches have been applied to the applicable equipment and that a commercial antivirus software product is installed and all of the latest signatures have been applied. Vendor shall be responsible for any costs, losses, damages, or expenses incurred by Client because of the introduction of any malware to Client's Information Technology environment by Vendor.

7. **Incident Response Requirements**: Vendor agrees to notify Client in writing immediately (and in any event within twenty-four (24) hours) whenever: (a) Vendor reasonably believes or suspects that there has been a Security Breach or (b) Vendor or Vendor Personnel may have been, or are likely to be, involved in unauthorized or illegal activities to obtain money or information from or through Client, Vendor's other clients or suppliers or in any way damage (or expose to damage) Client, Vendor's other clients or suppliers ((a) and (b) a collectively, "**Breach**"), and will thereafter diligently and continuously investigate the Breach, take all necessary steps to eliminate or contain the exposures that led to such Breach, and keep Client advised of the status of such Breach and all matters related thereto. Vendor shall collect, preserve and document all evidence regarding the discovery and cause of, and vulnerabilities, response, remedial actions and impact related to the Security Breach using means that shall meet reasonable expectations of forensic admissibility. Vendor further agrees to provide, at Vendor's sole cost, reasonable assistance and cooperation requested by Client and/or Client's designated representatives, in the furtherance of any correction, remediation, mitigation of any potential damage, and/or investigation of any such Breach and/or the mitigation of any damage, including any notification that Client may determine

appropriate to send to individuals impacted or potentially impacted, and/or the provision of any credit reporting service that Client deems appropriate to provide to such individuals. To the extent permitted by law, Vendor shall not notify law enforcement, any individual or any third party of any unauthorized access or acquisition of the Client data without first consulting with, and obtaining the written permission of, Client. Vendor agrees that Client, in addition to any other available remedies, shall have the right to seek an immediate injunction and other equitable relief in the event of any Breach, without the necessity of posting any bond or other security. In addition, within 30 days of identifying or being informed of a security exposure, Vendor shall develop and execute a plan, subject to Client's approval, that eliminates the exposure.

8. **User Activity Logs**: Vendor shall maintain logs of user activity for a minimum of 90 days for use in any investigation. These logs should include information such as user identification, date and time of activity, and details of the activity performed. The logs shall be made available to the Client upon request for the purpose of conducting an investigation and or an Audit conducted pursuant to Section 11 below.

9. **Independent Audit Report**: Vendor shall (a) maintain a secure environment for the Services that undergoes examinations from an independent auditor in accordance with the American Institute of Certified Public Accounts SSAE 18 (i.e. SOC 1) and the AICPA Trust Services Principles Section 100a, Trust Services for Security, Availability, Processing Integrity, Confidentiality and Privacy (i.e. SOC 2), and (b) provide Client with a copy of the foregoing examination report. Such audit and the report resulting therefrom shall cover, without limitation, Vendor's provision of the Services for a period of at least twelve months.

10. **Disaster Recovery**: During the term of this Agreement, Vendor shall maintain a disaster recovery plan which provides for the restoration of the Services within 24 hours of a failure (the "**Disaster Recovery Plan**"). Vendor shall test the Disaster Recovery Plan annually to confirm restoration is complete and accurate and provide Client with documentation of results. In the event any test of the Disaster Recovery Plan does not confirm a complete and accurate restoration, Vendor shall promptly correct such deficiency within thirty (30) days following notice from Client. If Vendor does not correct any such deficiency within such thirty (30) day period, Client may, in addition to any other rights or remedies available in law or at equity, terminate this Agreement at no cost or expense to Client.

11. **Right to Audit**: Upon reasonable notice to Vendor, Client will have the right to audit Vendor and Vendor Personnel to ensure that Vendor is providing the Services in the manner required by the terms of this Agreement, including the privacy and data security provisions set forth herein. Each party shall pay its own costs associated with such audit.

In connection with any such audit, Vendor shall provide Client (or its auditors) sufficient access to the Vendor system, software, facilities, equipment, policies, procedures, and records used in connection with the provision of the Services to perform the audit. Vendor shall provide Client (or its auditors) any and all reasonable assistance in connection with such audit. Client shall take reasonable steps to ensure that such audits do not interfere with Vendor's day-to-day operations. In the event Client (or its auditors) discovers any deficiency during any such audit, Vendor shall promptly correct such deficiency within thirty (30) days following notice from Client. If Vendor does not correct any such deficiency within such thirty (30) day period, Client may, in addition to any other rights or remedies available in law or at equity, terminate this Agreement at no cost or expense to Client.

12. **Standard Information Gathering Questionnaire**: In addition, upon Client's request, Vendor will complete and/or update the previously completed standard information gathering questionnaire required by Client and cause Vendor Personnel who access Client data to do the same, provided, that Vendor shall not be required to complete and/or update such questionnaire more than once in any twelve (12) month period. For the avoidance of doubt, the completion and/or update of such questionnaire shall not constitute an audit under this paragraph and shall not limit Client's right to audit Vendor as permitted above.

13. **Single Sign-On**: Vendor shall ensure that the Services are enabled for single sign-on to Campbell's reasonable satisfaction. Vendor represents and warrants that the Services are configured to accept the SAML 2.0 federation protocol and that the Services support both Campbell (IDP) and Vendor initiated sign-on. Vendor agrees to digitally sign the appropriate SAML assertion and/or response, as applicable, and comply with all of Campbell's reasonable requests related to single-sign on.

14. **Subcontractors**: Vendor shall not subcontract any portion of the Services without Client's prior written consent. In the event Vendor is permitted to subcontract any of its obligations hereunder, Vendor will remain primarily liable for the performance of the Services and will ensure that such subcontractors comply with each of the terms and conditions of this Agreement, including without limitation, the data security obligations set forth herein.

15. **Publicity**: Vendor may not use Client's name or disclose the terms or existence of this Agreement to any third party, including on Vendor's customer lists, press releases or otherwise, without Client's express prior written consent in each and every instance. In addition, all such press releases or the use of Client's name or any trademark of Client will require prior written approval by Client's Department of Global Communications.

16. **Data Breach Indemnity**: In addition to the requirements in the Agreement, Vendor shall indemnify Client for all costs, expenses, damages, losses, and liabilities associated with any data Breach.

17. **Artificial Intelligence Restrictions**: Vendor shall not use any artificial intelligence system, platform or tool to access, process, or analyze the Client data without Client's prior written consent. In the event Vendor is permitted to use any such system or tool for any one use case, Vendor shall ensure that (a) the Client data is encrypted at rest and in transit, (b) the system or tool does not retain, store, or disclose the Client data to any third party, (c) the system or tool does not use the Client data for any purpose other than providing the Services, and (d) the system or tool does not use or input the Client data to train, improve, or enhance any large language models or other machine learning algorithms that are owned or controlled by Vendor or any third party. Vendor shall also comply with the data provenance principles set forth below with respect to any such system or tool. For any Artificial Intelligence approved for use in support of the Services, Vendor shall provide an artificial intelligence bill of materials that is a comprehensive document that outlines the components and common algorithms used with the model built for the purposes and use of the model (the "**AI BoM**"). The AI BoM should include hardware, descriptions of models and methodologies, and any third-party tools, data sources, libraries, or frameworks integrated into the system.

18. **Data Provenance Principles**: In the event Vendor is permitted to use any artificial intelligence system, platform or tool to access, process, or analyze the Client data for any single use case, Vendor shall ensure that such system, platform or tool adheres to the following principles of data provenance: (a) the system, platform or tool shall record and document the sources, origins, and lineage of the data, as well as any transformations, modifications, or derivations applied to the Client data, in a transparent and traceable manner, (b) the system, platform or tool shall maintain the integrity, quality, and accuracy of the Client data throughout its lifecycle, and prevent any corruption, tampering, or loss of the Client data, (c) the system, platform or tool shall enable the verification, validation, and auditing of any use of the Client data, including, but not limited to, its processing by the system, platform or tool, and provide any relevant information or evidence upon request by the Client or any authorized third party. Artificial Intelligence shall mean any software that uses the Client Data in conjunction with any machine learning, neural network, deep learning, predictive analytics, large language model or other artificial intelligence computer or software program; or uses or attempts to use any deep-link, scraper, robot, bot, spider, data mining, computer code or any other device, program, tool, algorithm, process or methodology to systematically access, acquire, copy, download, extract or monitor any portion of the Client Data.