Schedule 2

Security Addendum

DEFINITIONS

Sysco Data: any data or information that is (a) loaded, submitted, or otherwise input into the Services or otherwise provided or transmitted to Supplier by or on behalf of Sysco Corporation and/or any of its Affiliates ("Sysco"); or (b) generated, reported, summarized, or otherwise output by the Services based on such data or information.

Sensitive Data: Personal Data; financial data, such as credit card numbers; banking information, such as bank account and routing numbers; compensation details; tax information; medical records; individual-specific dietary requirements; and Credentials and other user IDs and passwords.

Sysco Information Systems: any workstation, file server, applications, portable computer system, mobile computing device or other computer system, any network of such systems or machines, or any electronic data storage device or media owned, leased, or operated by or on behalf of Sysco Corporation and/or any of its Affiliates.

Supplier Information Systems: any computer system, Supplier Software, network, including but not limited to workstations, servers, mainframes, routers, switches, wireless networks, portable computer systems, mobile devices, software programs, and electronic storage media owned, leased or licensed by or operated on behalf of Supplier, and which accesses, stores or enables access to Sysco Data or has interconnected access to Sysco Information Systems.

1. INFORMATION SECURITY PROGRAM

Suppliers shall maintain a written information security program, policies, standards, and processes to ensure the security and resilience of the Supplier's products and services, and to maintain compliance with applicable laws and industry standards. The program shall ensure the confidentiality, integrity, and availability of Sysco Data in the Supplier's possession or control and to any Supplier Information Systems with access to Sysco Information Systems.

2. ACCEPTABLE USE OF ASSETS

(a) Suppliers must implement the appropriate security controls and take the appropriate protective measures while accessing Sysco Information Systems or Sysco Data.
(b) Sysco has the right to monitor activity on its systems, including internet and email use, to ensure systems security and effective operation, and to protect against misuse.
(c) Any monitoring will be carried out in accordance with audited, approved internal processes, and local data security and privacy laws (e.g., GDPR, CCPA).
(d) Sysco Data shall be accessed, used, or shared only to the extent it is authorized and necessary for Supplier to deliver the specifically contracted service to Sysco.
(e) Sysco Data shall remain on Sysco Information Systems. Prior written authorization from Sysco Cybersecurity is required before Sysco Data can be shared or transferred to the Supplier or subcontractors.

(f) All Suppliers are held accountable for their actions on the Sysco Information Systems that is accessed and must not:

- Allow unauthorized use of their login credentials on any Sysco Information System
- Leave their user accounts logged in and unattended and system access to an unlocked computer
- Use someone else's user ID and password
- Leave system and application passwords unprotected or unencrypted (e.g., Writing it down)
- Perform any unauthorized changes to Supplier or Sysco Information Systems or Sysco Data
- Attempt to gain access to unauthorized Supplier or Sysco Information Systems or Sysco Data
- Access, store or transmit Sysco Data to any person or organization without the appropriate approval
- Expose any Sysco proprietary information on an unmonitored device or in an uncontrolled manner (e.g., printer, desk)
- Violate any sensitive intellectual property, copyright, or trade secrets
- Connect Supplier and Sysco issued devices to unsecured Wi-Fi networks

3. APPLICATION SECURITY

(a) No license is granted to Supplier, either expressly or by implication, or license to access or use for any purpose any Sysco Data, Sysco Information Systems, or any software in Sysco's computing environments.

(b) Supplier shall not attempt to copy, alter, decompile, reverse engineer, or disassemble any of the software programs contained in Sysco Information Systems. If the services include the development of software product(s), including web applications, for Sysco, such software shall be developed and maintained in accordance with the development methodology specified by Sysco. Such software shall satisfy the appropriate Sysco information security policies and guidelines that are furnished by Sysco to Supplier (which are incorporated herein by reference).

(c) Supplier shall comply with any instructions, guidelines or minimum compliance controls that are furnished by Sysco to the Supplier to enable Sysco to comply with other applicable laws and regulations.

(d) To the extent that Supplier uses internally developed software or web applications to provide the Services, even if such items are not developed exclusively for Sysco, then:

- Supplier shall ensure that such items comply with any instructions, guidelines or minimum compliance controls that are furnished by Sysco to Supplier to enable Sysco to comply with applicable laws and regulations, and
- Supplier will provide Sysco with such information as is reasonably necessary for Sysco to confirm that applicable compliance controls are in place.

(a) Supplier shall maintain the security of Supplier applications servicing Sysco or hosting Sysco Data with appropriate application security controls, including but limited to:

- Secure systems development processes
- Access to external-facing applications must be filtered through firewalls
- Components of application architecture must be separated into different tiers according to their function
- Databases must not be hosted on the same host as the application web server

- Undergo application security testing, i.e., static application security testing, dynamic application security testing, and provide test results to Sysco as requested.

4. ASSET IDENTIFICATION

(a) Supplier must ensure that all Sysco Data shared by Sysco should be classified according to its level of confidentiality, sensitivity, value, and criticality.
(b) Sysco Data should be classified, protected, and handled in accordance with contractual requirements and applicable privacy policies, for continuous alignment with applicable privacy laws, regulations, standards, and industry best practices.
(c) All information assets should be protected in a manner commensurate with their classification.

5. DATA PROTECTION

(a) Supplier shall ensure that assets and systems use mechanisms (including cryptographic mechanisms) to prevent unauthorized disclosure of Sysco Data, including Sensitive Data and Personal Data stored at rest.
(b) Supplier must protect Sysco Data in compliance with all applicable regulatory requirements.
(c) No Sysco Data may be accessed, generated, hosted, downloaded, printed, stored, processed, transferred, or maintained by Supplier in countries or locations outside of the United States without Sysco's prior written approval. Such approval may be withheld by Sysco for any reason in its sole discretion and/or approval may be subject to additional terms and conditions.
(d) Sysco approved encryption technology should be used to encrypt Sysco Data at rest, including file level encryption.
(e) Sysco Data should be file-level encrypted and transmitted with an encrypted protocol.
(f) Supplier must employ encryption solutions which comply with current industry standards. The encryption solution chosen should meet the following minimum requirements:
    - Uses public/private key pairs
    - Uses a minimum of 256-bit key encryption
    - Uses a strong password that comply with current industry standards
    - Sysco maintains the right to prohibit the use of insecure encryption technologies when accessing Sysco Information Systems
(g) Supplier shall maintain such encryption for all transmissions by Supplier of Sysco Data via public networks (e.g., the Internet). Such transmissions include, but are not limited to:
    - Sessions between web browsers and web servers
    - Email containing Sysco Data (including passwords)
    - Transfer of files via the Internet (e.g., FTP)
(h) Supplier shall protect keys and key materials from unauthorized disclosure
(i) Supplier will ensure that they obtain prior written authorization from the Sysco Business Owner and Cybersecurity team to use Sysco Data for other than its intended purpose (e.g., in a manner different from the original intent/business purpose).
(j) Where Sysco Data is copied from the Supplier's production environment for the purposes of conducting tests the Supplier shall:
    - Implement an authorization process to review and approve
    - Require separate authorization each time Sysco Data is copied from production into the testing environment

- Log the use of Sysco Data

(k) Sysco Data must be retained only for the duration of time required to deliver the specifically contracted service to Sysco, after which it must be destroyed or safely returned to Sysco.

6. CLOUD SECURITY

(a) Supplier shall not utilize (nor permit any subcontractor) access to shared hosting or virtualized "cloud" hosting resources in support of Sysco without Sysco's prior written notification. Supplier shall provide Sysco with 30 days notification. Sysco may terminate this Agreement with reasonable notice.

(b) Supplier shall not store or aggregate (nor permit any subcontractor to store or aggregate) Sysco Data (including, for example, program code, database scripts, data extracts, process flows, calculations, macros, and business logic) in a shared (co-mingled) environment, including cloud computing environments, databases, data warehouses or data analytics environment, without written approval from Sysco.

(c) Supplier shall physically and/or logically segregate Sysco Data from data of other Supplier customers.

(d) Supplier virtual systems and services associated with cloud solutions providing services to Sysco or hosting Sysco Data shall be deployed and configured securely.

7. ENDPOINT AND SECURITY HARDENING

Supplier shall maintain industry standard capabilities to protect Sysco Data from theft, loss, or unauthorized access, to include:

- Endpoint security software must be installed and active on all Supplier Information Systems.
- Anti-virus installed must not only detect viruses but also should be able to detect malicious code; provide safe internet browsing in browsers; anti-virus software agents must always be able to communicate with the anti-virus server to install signature updates when available.
- Industry recognized hardened system images (i.e., CIS benchmarks) installed on all Supplier Information Systems.
- Full disk encryption on all Supplier Information Systems
- Content aware solution (i.e., data loss prevention) to discover, monitor, and protect Sysco Data during transit/at rest across all Supplier Information Systems.
- Processes for becoming aware of and maintaining security patches and fixes to minimize security vulnerabilities

8. HUMAN RESOURCE AND PERSONNEL SECURITY

(a) Depending on the geographical location and where local law permits, Supplier shall be responsible for performing criminal background checks on, hiring, and employing personnel in compliance with applicable laws.

(b) Background checks of all personnel must be completed as an initial verification check before hiring by the respective HR leads, depending on geographical location and where local law permits.

(c) Sysco may reasonably request, and Supplier shall provide to Sysco, confirmation that adequate background checks have been completed on the personnel hired in accordance with applicable laws depending on geographical location and where local law permits.
(d) Supplier shall have an information security training and awareness program to periodically educate and inform Supplier personnel of security threats, best practices, and how to keep data and information systems secure.

9. IDENTITY AND ACCESS MANAGEMENT

(a) Identification and Authentication

i. All access to any Sysco Data shall be Identified and Authenticated as defined in this Section.
   - "Identification" (or "Identify," as the context requires) refers to processes which establish the claimed or purported identity of the person or entity requesting access to Sysco's Information Systems.
   - "Authentication" (or "Authenticate," as the context requires) refers to processes which validate the purported identity of the requestor.

ii. For access to Sysco's information systems Supplier shall require the following:
   - The provision of Identification by the requestor (i.e., no anonymous account may request information); and
   - Authentication of the requestor using an individual, unique user ID and an individual password or other appropriate Authentication technique approved by Sysco in writing.

iii. Supplier shall enforce industry standard multi-factor authentication (MFA) for high-risk transactions impacting Sysco Data and applications that stores or transmits Sysco financial data.
iv. Supplier shall maintain procedures to ensure the protection, integrity, and soundness of all passwords created by Supplier and/or used by Supplier in connection with the Agreement.

(b) Account Administration

i. Supplier shall maintain appropriate processes for requesting, approving, and administering accounts and access privileges, including privileged access, for Sysco Information Systems and Sysco Data. These processes shall be required for both Sysco-related accounts and Supplier's internal accounts and shall include procedures for granting and revoking emergency access to Sysco's Information Systems.
ii. All access by Supplier Personnel to Sysco Information Systems shall be subject to prior approval by Sysco and shall follow Sysco's access standards and procedures.

(c) Access Control

i. Supplier shall maintain appropriate access control mechanisms to prevent all access to Sysco Information Systems and Sysco Data except by (a) specified users expressly authorized by Sysco and (b) Supplier Personnel who have a "need to know access" to perform a particular function in support of Supplier Processing. The access and privileges granted shall be limited to the minimum necessary to perform the assigned functions.
ii. Supplier shall maintain processes to ensure that Supplier Personnel with access to Sysco Information Systems and Sysco Data is revoked no later than two business days upon termination and immediately in the case of involuntary termination.
iii. Supplier shall maintain appropriate mechanisms and processes for detecting, recording, analysing, and resolving unauthorized attempts to access Sysco Information Systems and

Sysco Data. If Supplier Personnel change roles or for any other reason no longer requires access to Sysco Information Systems, Supplier will notify Sysco within three business days. In the case of involuntary termination, Supplier will notify Sysco within 24 hours.

(e) **Access Auditing**

Supplier shall maintain appropriate access audit mechanisms to ensure that all instances of access to Sysco Data are specifically identified by a recording of each of

(i) the Identity of the person accessing the information,
(ii) the time of access,
(iii) the method of access, and
(iv) what data was accessed. Supplier shall maintain complete access audit logs for at least 12 months.

10. REMOTE ACCESS

(a) Unauthorized devices and/or software should not be used to facilitate remote access to Supplier Information Systems.
(b) Multi-factor authentication shall be required to remotely access the Supplier's information technology environment.

11. PATCH AND VULNERABILITY MANAGEMENT

(a) Supplier must apply all relevant Supplier security patches to Supplier Information Systems according to the following schedule:
    i. Critical or High rated patches applied within 30 days of release date
    ii. Medium rated patches must be applied within 90 days of release date
(b) Supplier must use a vulnerability scanning tool that complies with industry standards in order to validate security of Supplier Information Systems.
    i. External scanning must occur quarterly.
    ii. Internal scanning must occur once every six months.
    iii. Critical or High rated vulnerabilities must be addressed within 30 days of discovery.
    iv. Medium rated vulnerabilities must be addressed within 90 days of discovery.
(c) An application penetration test must be performed by a certified professional annually and after any significant change in the network and/or systems
    i. Critical or High rated vulnerabilities must be addressed within 30 days of discovery.
    ii. Medium rated vulnerabilities must be addressed within 90 days of discovery.
(d) Supplier shall provide at Sysco's request the results of external vulnerability testing, internal infrastructure vulnerability testing, and application vulnerability testing.

12. LOGGING AND MONITORING

Suppliers information systems must generate logs with sufficient details and store them for an appropriate time, to include but not limited to the following:

(a) Generate event logs containing information establishes the following: the type of event; when and where the event occurred; the source of the event; outcome of the event; and the identity of any users associated with the event.
(b) Generate systems and applications logs and be readily available for at least 13 months from the date of generation.

(c) For each logged event, the audit log must contain, but not be limited to, the following information depending on the type of event:
    - The user's ID, by which the program was operating
    - System activity (e.g., create a file, login/logout, etc.)
    - Date of event
    - Time of event
    - Device identity or location and system identifier (IP Addresses, DNS Name, MAC addresses, Ports)
    - Remote log-in attempts if any
    - Records of successful and rejected system access attempts
    - Records of successful and rejected resource access attempts
    - System configuration changes
    - Use of privileges
    - Network addresses and protocols

(f) Alarms raised by the access control system in case event logs contain personally identifiable information, appropriate privacy control measures per the local law and global regulations must be taken.

(g) Protect log files through their lifecycle and analyse the logs for timely monitoring and alerting (in case of a security event) for safeguarding Sysco Information Systems and Sysco Data.

(h) Monitor systems and analyse logs timely for any suspicious activity.

13. NETWORK SECURITY

(a) Supplier shall only have access to Sysco's Information Systems authorized by Sysco and shall use such access solely for providing Services to Sysco.

(b) Supplier shall not attempt to access any applications, systems, or data which Sysco has not authorized Supplier to access, or which Supplier does not need to access to perform services for Sysco.

(c) Supplier further agrees to access such applications,data, and systems solely to the extent minimally necessary to provide Services to Sysco. Supplier's attempt to access any applications, data, or systems in violation of the terms in this Section shall be a material breach of the Agreement.

(d) Supplier shall provide at Sysco's request applicable network diagram(s) that outline Supplier's information technology network infrastructure, and all equipment used in relation to providing the Services or otherwise fulfilling Supplier's obligations under this Agreement, including:
    - Connectivity to Sysco and all third parties who may access Supplier's network to the extent the network contains Sysco Data;
    - All network connections including remote access services and wireless connectivity;
    - All access control devices (for example, firewall, packet filters, intrusion detection, and access-list routers);
    - All back-up or redundant servers; and
    - Permitted access through each network connection.

14. MOBILE DEVICE MANAGEMENT

(a) Supplier shall ensure the Supplier Personnel will not be permitted to, and will not, utilize personal computing equipment for accessing Sysco Information Systems or processing Sysco Data.
(b) Supplier shall monitor and prevent Sysco's Data from being sent via social media or personal email accounts. Sysco Data must not be copied, replicated, or synchronized with personally owned mobile devices unless the device has security controls implemented by Sysco and complies with all applicable standards.
(c) Supplier shall restrict access to, and the use of removable media, such as USB ports, writable optical media, portable hard drives, and other removable media.

15. SECURITY INCIDENT MANAGEMENT

(a) Supplier shall maintain a documented data breach action and response plan.
(b) Supplier shall notify Sysco of a Security Incident as soon as practicable, but no later than twenty-four (24) hours after Supplier becomes aware of it. Supplier shall send notifications to cyber@sysco.com. Immediately following Supplier's notification to Sysco of a Security Incident, the parties shall coordinate with each other to investigate the Security Incident. "Security Incident" means any act or omission that compromises either the confidentiality, integrity, or availability of Sysco Data or the physical, technical, administrative or organizational safeguards that relate to the protection of the confidentiality, integrity, or availability of Sysco Data.
(c) Supplier will cooperate with any investigation led by Sysco or law enforcement.
(d) Supplier will not disclose suspected or confirmed Security Incidents involving Sysco Data to any third party without the prior written approval of Sysco, except to the extent such disclosure is required by applicable law.
(e) Supplier shall be solely responsible for the costs of remedying any Security Incidents caused by a breach by Supplier of its obligations under the Agreement, including the cost to provide any notices to affected third parties, to purchase credit monitoring services for such third parties, and to provide customer or employee support to such third parties (e.g., call centre services to receive inquiries from affected third parties).

16. SUPPLIER / SUPPLIER IT RISK

(a) The Supplier must complete the required Sysco Cyber due diligence and remediate identified findings prior to commencing service to Sysco.
(b) At Sysco's written request, Supplier shall promptly and accurately complete a written information security questionnaire provided by Sysco regarding Supplier's security practices and information technology environment as related to Services provided under this Agreement. Sysco will not request a security questionnaire more frequently than once per year unless:
    i. There has been a security breach with respect to the Services or a complaint regarding Supplier's privacy or security practices; or
    ii. Sysco has reason to believe there are material changes in the information provided by Supplier in response to the most recent security questionnaire.
(c) A contact person within the Supplier's organization must be accountable during the whole contract lifecycle to ensure that:
    - Security risks and requirements are fully understood;
    - Appropriate processes are in place and a minimum acceptable level of residual risk is agreed with the provider and duly accepted by each party; and

- Security risks are managed, and appropriate processes are in place and communicated

(i) The Supplier must provide information regarding existing and/or potential subcontractors (or any fourth parties) used to provide products and services to it or in turn to Sysco as stated in the Agreement.

(j) The subcontractor must comply with the same or equivalent security standards as the ones applied to the Supplier.

(k) Sysco Data must not be shared with any fourth party without prior consent and approval from Sysco.

(l) The Supplier must provide documentation of its business continuity and disaster recovery plan and testing.