Business Award Letter - DATA SAFEGUARDS Requirements

1. Supplier shall have and maintain an effective information security program that encompasses administrative, technical, and physical safeguards that meet or exceed the requirements specified in applicable industry standards (e.g., ISO 27001, NIST CSF) to protect against a disruption of the supply of Product, and threats to the unauthorized or accidental destruction, loss, alteration, or use of Buyer information (or that of its affiliates, collectively "**Buyer Information**").

    1.1. If Supplier intends to implement a change to its information systems, policies or procedures that would reduce the level of information security safeguards in place as of the Effective Date of the Award Letter, Supplier shall notify Buyer.

    1.2. Supplier shall identify requirements for, and institute and practice, a Business Continuity and Disaster Recovery Plan (the "**Plan**") that will prevent catastrophic data and/or operations loss and resume operations timely in the event of system failure, damage, or destruction, to ensure fulfillment of Products and services to Customer. Supplier shall ensure the Plan is tested no less frequently than once every two years to ensure it can be executed correctly and efficiently.

    1.3. For the protection of classified Buyer information or sensitive personal information, Supplier shall implement data encryption using strong, non-proprietary cryptographic protocols that are consistent with those standards set forth in the current versions of the FIPS 140 series, the NIST Special Publication 800 series or ISO 27001 requirements.

    1.4. Supplier shall allow and support the completion of periodic assessments by Buyer or a Buyer affiliate to determine compliance with these information security requirements.

2. If Supplier personnel are provided ongoing access to Buyer's facilities and/or network and computing resources, they shall abide by all applicable Buyer Acceptable Use policies, and complete Buyer information security training. Supplier's access or connectivity may be terminated at any time upon violation of Buyer's policies and/or misuse or abuse of Supplier's privileges.

3. Supplier shall have and maintain a formal information security incident monitoring, reporting and response capability to identify, report and appropriately respond to known or suspected information security incidents, including any unauthorized access, acquisition, use, disclosure, or destruction of Buyer information.

4. If Supplier discovers or is notified of a breach of security relating to Buyer information or that would otherwise interrupt, degrade or compromise the integrity of services provided to Buyer, or interrupt the supply of Products, Supplier shall; (a) notify Buyer within 48 hours of such breach; and (b) if Buyer information was in the possession of Supplier at the time of such breach, Supplier shall; (i) promptly investigate and remediate the effects of the breach; and (ii) provide Buyer with satisfactory assurance that such breach will not reoccur.

5. No Buyer information shall be sold, assigned, leased, or otherwise disposed of to a third party, or commercially exploited, by or on behalf of Supplier or its personnel without Buyer's express written consent. Supplier shall not collect, share, disclose or use any Buyer information except as necessary to perform the services and supply the Products described in the Agreement, and shall not use Buyer data or Buyer confidential information in Gen AI solutions without the express written consent of Buyer. For the purposes of these Data Safeguard Requirements, "**Gen AI**" means a category of artificial intelligence (AI) algorithms that generate new outputs based on the data on which they have been trained, including, but not limited to, ChatGPT, Promethean AI, Google Gemini, Baidu Ernie and

Microsoft Copilot 365. Notwithstanding the foregoing, and provided Supplier does not use Buyer's information, intellectual property rights, or confidential information for training an AI model, nothing shall prevent Supplier, and Supplier shall not require any prior Buyer consent, in relation to the use by Supplier of Artificial Intelligence tools (Supplier's own proprietary tools or external provided tools) for the purposes of Supplier's own internal use and not for the use on behalf of Buyer. Furthermore, Supplier represents and acknowledges that it does not receive, nor is Buyer providing, any such Buyer information in consideration for the provision of the services or otherwise. Supplier additionally represents and warrants that the provision of the Services shall comply with applicable data protection laws.