1. PERSONALLY IDENTIFIABLE INFORMATION PROTECTION (Clause F-7.1) (November 2021)

Definitions.

a. "Buyer Personally Identifiable Information " means Personally Identifiable Information:
   (i) provided to Seller by or on behalf of Buyer;
   (ii) from any source processed by Seller on behalf of Buyer;
   (iii) from any source pertaining to Buyer personnel; and,
   (iv) created by Seller based on data in section (i), (ii) or (iii) above.

b. "Personally Identifiable Information (PII)" means any information about an individual, including but not limited to, education, financial transactions, medical history, criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

c. "Security Breach" means any event involving an actual, suspected or alleged compromise of the security, confidentiality or integrity of Buyer PII. It includes but is not limited to any accidental, unauthorized or unlawful destruction, use, loss, alteration, or disclosure of or access to Buyer PII.

Processing for Limited Purposes. Seller shall process Buyer PII in accordance with Buyer's written instructions (which include any means capable of visual display and retention) and only to the extent necessary to perform this Purchase Order/Contract. Seller shall restrict access to Buyer PII to its staff who need access to the PII to perform their job functions.

Third Parties. Seller shall not disclose Buyer PII to any third party unless it receives Buyer's prior permission in writing or via telephone, email, or other electronic means.

Legal and Regulatory Compliance. Seller shall comply with all laws and regulations that apply to the processing and protection of Buyer PII.

Security. Seller shall adopt appropriate technical and organizational measures to protect Buyer PII against accidental, unauthorized or unlawful processing, destruction, loss, alteration, disclosure and access, in particular where processing involves the transmission of Buyer PII over a network, and against all other unlawful processing. These technical and organizational measures shall comply with applicable data protection laws and regulations and shall have regard to the state of the art, cost of implementation, nature of Buyer PII, and the risks to which the Buyer PII are exposed by virtue of human action or the physical or natural environment.

Response to Inquiries. Seller agrees that it will respond promptly and fully to all inquiries from Buyer or any supervisory authority regarding processing activities on Buyer PII. It will also respond promptly and fully to all inquiries from Buyer's employees concerning the processing by Seller of Buyer PII relating to him or her.

Return/Destruction of PII. After Buyer PII is no longer needed for the purposes set forth in this purchase order/contract, Seller will promptly return them to Buyer or, alternatively, destroy them, subject to any requirement upon Seller under applicable law to retain Buyer PII for a specified period of time.

Security Breach. Seller shall notify Buyer in the most expedient time possible under the circumstances and without unreasonable delay of any Security Breach involving any Buyer PII. As soon as such information can be collected or otherwise becomes available, Seller shall also provide Buyer with a detailed description of the Security Breach, the type of data that was the subject of the Security Breach, the identity of each affected person, and any other information Buyer may request concerning such affected persons and the details of the breach. Seller agrees to take action immediately, at its own expense, to investigate the Security Breach and to identify, prevent and mitigate the effects of any such Security Breach, and to carry out any recovery or other action necessary to remedy the Security Breach, including mailing notices to affected persons as may be required by applicable laws. The content of any filings, communications, notices, press releases, or

reports related to any Security Breach ("Notices") must first be approved by Buyer prior to any publication or communication to any third party. Seller shall pay for or reimburse Buyer for all costs, losses and expenses relating to any Security Breach, including without limitation, the cost of Notices or identity theft insurance and will indemnify, defend, and hold the Buyer harmless against third party claims (including, without limitation, the parties' employees) related to any Security Breach.

Seller's Staff. Seller shall implement all measures necessary to ensure compliance by its staff with the obligations relating to Buyer PII. Seller shall also require Seller's staff to sign individual confidentiality agreements that require protection of Buyer's PII.

Right of Access and Rectification. Seller shall notify Buyer within three (3) business days of any communication received from any Buyer employee relating to that employee's rights to access, modify or correct Buyer PII relating to him or her and shall comply with all instructions of Buyer in responding to those communications. In addition, Seller shall provide any and all assistance required by Buyer to respond, within the time period required by applicable law, to any communication received by either party from any Employee relating to that Employee's rights to access, modify or correct Buyer PII relating to him or her.

Audit. After providing prior written notice to Seller, Buyer may conduct at any time an on-site verification of Seller's compliance with obligations relating to Buyer PII, even after the termination of this purchase order/contract. Seller shall provide access to all concerned facilities, equipment and records to allow Buyer to conduct that verification.