SCHEDULE - INFORMATION SECURITY REQUIREMENTS

Contractor shall maximize the security of its people, processes, and technologies, and the people, processes, and technologies of each Seller and Subcontractor, throughout the term of the MGSA and all Purchase Orders entered into thereunder in accordance with the requirements set forth in this Schedule and all Applicable Laws (collectively, the "**IS Requirements**"). Company reserves the right to validate the effectiveness of the IS Requirements, and Contractor shall provide evidence of Seller, Subcontractor and other third-party independent validation.

Contractor is responsible for each Seller's and Subcontractor's compliance with the IS Requirements, and references to "**Contractor**" herein include each Buyer and Subcontractor. Similarly, references to "**Company**" herein include each Buyer.

The term "**Product**" as used herein means any service, equipment, systems, or software furnished by Contractor to Company hereunder.

Company may amend the IS Requirements from time to time upon written notification to Contractor.

1. Incident Response and Breach Notification

Contractor shall report any breach or any other security incident, whether internal or external, that compromises or has the potential to compromise the Product(s) or Services(s) to the Sempra Infrastructure's Cybersecurity Fusion Center (CFC@sempraglobal.com and +1(866) 734-3457 in the US or (800) 626-6126 in México) within 24 hours of its knowledge of the breach or incident. Thereafter, Contractor shall provide periodic status updates describing actions being taken to mitigate damage or otherwise respond. The first such update should occur no more than 72 hours after Contractor's initial notification to the Sempra Infrastructure's Cyber Fusion Center.

2. Encryption

Where Company determines that encryption is acceptable to prevent unauthorized disclosure of Company information, Contractor's Product(s) must contain cryptographic controls that satisfy the requirements of FIPS 197 such that Company's sensitive data and information is rendered inaccessible by an unauthorized user. Where Contractor's Product uses encryption keys, the Product must not store hard-coded encryption keys within the source code. Encryption keys must be stored and secured separately from the Product while in transit and while at rest and will be revocable for re-implementation and maintenance.

3. Data Security

3.1 In the event of a suspected or actual breach or compromise involving Contractor's infrastructure, whether or not in connection with a Product, Company may, in its sole discretion, block or restrict any and all methods and sources of Contractor's access, including communication, connectivity, and integrations (collectively, "Right to Block"). Notwithstanding any other Company requirement or obligation in the MGSA or any Purchase Order, if Company exercises its Right to Block, Company will have no liability to Contractor arising out of or otherwise connected in any manner thereto. Required Contractor access will only be restored after Contractor has effectively proven, via an independent and competent third party, that the Product and related systems no longer pose a potential or actual threat to Company.

4. Destruction

Contractor agrees that when the data retention period has been exceeded, the data is no longer required, or at the request of the Company, Contractor will destroy the data in a manner that will render it completely unusable and unrecoverable, and will provide Company with a certificate of destruction, upon Company's request.

5. Conflicts

Nothing contained herein shall be construed to limit any of Contractor's obligations regarding nondisclosure or information protection contained elsewhere in the MGSA and any Purchase Order.