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. Access Controls

1.1 Contractor shall provide role-based access, authorization, and accountability controls within their Product in relation to the Products which conform to the guidelines and requirements set forth in the IS Requirements. Controls must be appropriate for the sensitivity of the information.

1.2 Contractor shall provide for separate roles for day-to-day users, administrators, developers, and support staff with access to the Products, and such access must be limited only to authorized personnel who have been properly trained on administrative responsibilities and security process and procedures. Access control must provide the minimum access required for each role and deny access for unauthorized users.

1.3 Contractor's hosted Product must include controls for securing service accounts and generic accounts and prevent their unauthorized use. Service account and generic account passwords must be changed at least annually.

1.4 Contractor warrants that administrators for the hosted Product production environment will utilize two-factor authentication when providing remote administrative support for the environment.

2. Shared Architecture

Contractor shall identify where shared resources are utilized within its architecture by other clients and the security controls implemented to protect Company data from access by unauthorized users and third parties. Service contracts which include a dedicated environment must not contain shared resources including, but not limited to, all components, systems, and infrastructure.

3. 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.

4. 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.

5. Password and Logon Standards

5.1 Single sign-on must be used in any Products(s) and in connection with Company information systems whenever possible. If, in relation to any Product, single sign-on is not possible, Contractor shall provide Company notice thereof and ensure that that Product complies comply with CIS security implementation group level 2 (IG2) or higher pertaining to password and logon standards.

5.2 Without limiting any other provision of the MGSA or any Purchase Order:

(a) each Product must provide a unique ID (individually identifiable) for user accounts; and

(b) multi-factor authentication must be used to access systems and data which are either identified by Company as sensitive or confidential, or which should be reasonably understood by Contractor to be sensitive or confidential.

6. Data Security

6.1 Contractor certifies that its Products provide the necessary security to meet all Applicable Laws for storing, processing, and transmitting data. This specifically includes all laws and regulations that require specific protections for personally identifiable information, credit card and financial information, and audit records. Contractor shall allow third party validation of compliance with all legal and regulatory requirements.

6.2 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.

7. Logging and Errors Details

Contractor shall log all application usage, user access, misuse, and sufficiently detailed error messages for monitoring and analyzing the use of the Products and will retain all information for a minimum of 90 days from the log date. Contractor shall ensure that the Products include audit trails, time stamped log entries, and unique log identifications. Company has the right to request logs at any time and at no cost to Company.

8. Vulnerabilities and Defects

8.1 Contractor shall maintain a vulnerability and defect tracking process which reviews potential defects for the security impact to Contractor’s Product(s) and the components and software packages that support them at no cost to Company. Contractor shall, at Contractor’s expense, test and remediate for all publicly disclosed software vulnerabilities posted to the National Vulnerability Database (http://nvd.nist.gov/) and by the Open Web Application Security Project (www.owasp.org) within 30 days of posting. Generally, this will prevent Products from being easily susceptible to cross-site scripting, SQL injection, buffer overflows, input validation, and other similar attacks.

8.2 Contractor warrants that the Products will not contain any code that might facilitate unexpected or unapproved access or outages to the Products, including: computer viruses, worms, time bombs, backdoors, trojan horses, easter eggs, and other forms of malicious code, and shall provide documentation detailing such processes upon request by Company and at no cost to Company.

9. Third-Party Security Assessments and Testing

9.1 Contractor shall engage an independent third party ("Testing Company"), to be approved by Company, at Contractor's expense, to test Products for vulnerabilities through detailed security tests on an annual basis through an Industry Standard Certification (e.g., ISO 27001, SOC 2 Type 2, etc.). In lieu of an Industry Standard Certification, Contractor may elect to have the Testing Company perform an annual test of Information Security controls which support the Products, their Production hosting environment, and their operational support infrastructure.

9.2 Contractor shall require the Testing Company to provide a report detailing the results of the tests performed and shall provide a copy of such report to Company within 30 days of the applicable tests. If any such report shows vulnerabilities in the Products, Contractor shall promptly provide Company with a proposed remediation plan, with a timeline for completion, all at no cost to Company.

9.3 All Product vulnerabilities, defects, and bugs disclosed to Contractor shall be corrected and remediated by Contractor, at Contractor's expense, within 30 days from the date of the applicable Testing Company's report or the date on which Contractor becomes aware of such vulnerabilities, defects, or bugs.

10. Right to Report

Company may report, to one or more public vulnerability reporting organizations, any defects or configuration conditions which result in vulnerabilities contemplated in these IS Requirements, if such defects or configuration conditions are not resolved or otherwise fixed within 90 days of discovery or earlier if agreed upon by both Company and Contractor. Nothing contained in the IS Requirements will be construed to limit any of Contractor's other obligations regarding nondisclosure or information protection described in the MGSA and any Purchase Order.

11. 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.

12. Formal Documentation

Contractor agrees to provide formal documentation for the use, maintenance, and secure implementation of Contractor's Product. Product documentation will be updated within thirty (30) days of a Product update, upgrade, patch, or similar change. Product documentation will include an inventory of all components, configurations, and dependencies.

13. 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.