**SCHEDULE I**

***Information Security Requirements***

Contractor agrees to maximize the security of its people, processes, and technologies throughout the term of this Agreement in accordance with the requirements set forth in this Schedule and all applicable laws (collectively, the “IS Requirements”). Company shall be permitted to amend the IS Requirements upon written notification to Contractor. The term “product” as used herein means any service, equipment, system, or software furnished by Contractor to Company hereunder.

1. **Access Controls**

Contractor will provide role-based access, authorization, and accountability controls within their product which conform to the guidelines or requirements set forth in the IS Requirements. Controls must be appropriate for the sensitivity of the information. In addition, the product will provide for separate roles for day to day users, administrators, developers, and support staff, and that the access shall provide access to authorized personnel only who have been properly trained on administrative responsibilities and security process and procedures. Access Control shall provide the minimum access required for each role and deny access for unauthorized users. Contractor’s hosted product will 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. Contractor further warrants that administrators for the hosted product production environment will utilize two-factor authentication when providing remote administrative support for the environment.

1. **Shared Architecture**

Contractor will 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 shall not contain shared resources including, but not limited to, all components, systems, and infrastructure.

1. **Incident Response and Breach Notification**

Any breach or any other security incident, internal or external that compromised or has the potential to compromise the product(s) must be reported to the Sempra Energy Security Operations Center (SOC@sempra.com and (858) 613-3278) within 24 hours of knowledge thereof followed by periodic status updates to describe actions being taken to mitigate damage and otherwise respond. These updates should occur no more than 72 hours from Contractor’s initial notification to the Sempra Energy Security Operations Center.

1. **Encryption**

Where Company determines that encryption is acceptable to prevent unauthorized disclosure of Company information, in order to protect Company sensitive information, Contractor’s product(s) will use 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, Contractor’s product will not store hard-coded encryption keys within source code. Encryption keys will be stored and secured separately from the product while in transit and while at rest and will be revocable for re-implementation and maintenance.

1. **Password and Logon Standards**

Even if no other provision of this Agreement requires single sign-on, it must be used in any products(s)and/or in connection with Company information systems whenever possible. Only under those circumstances where no other provision of this Agreement requires single sign on, if single sign-on is not possible, Contractor shall provide Company notice thereof and the product(s)will comply with CIS security implementation group level 2 (IG2) or higher pertaining to password and logon standards. Without limiting the foregoing, the product(s) will provide a unique ID (individually identifiable) for user accounts. In addition, without limiting any other provision of this Agreement, multi-factor authentication must be used to access systems and/or 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**

a. Product Security Certification. Contractor certifies that their product provides the necessary security to meet all applicable laws and regulatory requirements for storing, processing, and transmitting data. This specifically includes, but is not limited to, all laws and regulations that require specific protections for personally identifiable information, credit card and financial information, and audit records. Contractor agrees to allow third party validation of compliance with all legal and regulatory requirements.

b. Ability to Block/Restrict. In the event of a suspected or actual breach or compromise involving the Contractor's infrastructure, whether or not in connection with the product, Company may, in its sole discretion, block or restrict any and all methods and sources of Contractor’s access, including without limitation, communication, connectivity and integrations (collectively, “Right to Block”). Notwithstanding any other Company requirement or obligation in this Agreement, if Company exercises its Right to Block, Company shall have no liability to Contractor arising out of or otherwise connected in any manner thereto. Required Contractor access shall only be restored after Contractor has effectively proven via an independent and competent third party that their product and related systems are no longer pose a potential or actual threat to Company.

1. **Logging and Errors Details**

Contractor agrees to log all application usage, user access, misuse, and sufficient detailed error messages for monitoring and analyzing the use of the product and will retain all information for a minimum of ninety (90) days from the log date. Contractor further agrees that the product includes an audit trail, time stamped log entries, and unique log identification. Company has the right to request logs at any time and at no cost to Company.

1. **Vulnerabilities and Defects**

Contractor agrees to maintain a vulnerability and defect tracking process which reviews potential defects for their security impact to Contractor’s product(s) and the components and software packages that support it at no cost to Company. Contractor further agrees, at Contractor’s expense, to test and remediate for all publicly disclosed software vulnerabilities posted to the National Vulnerability Database (http://nvd.nist.gov/) and by Open Web Application Security Project (www.owasp.org) within thirty (30) days of being posted. Generally, this will prevent the product from being easily susceptible to cross-site scripting, SQL injection, buffer overflows, input validation, and other similar attacks. Contractor further warrants that the product shall not contain any code that may facilitate unexpected or unapproved access or outages to the product, including, but not limited to: computer viruses, worms, time bombs, backdoors, trojan horses, easter eggs, and other forms of malicious code, and agrees to provide documentation detailing such processes upon request by and at no cost to Company.

1. **Security Assessments and Testing**

Contractor agrees that it will engage an independent third party, to be agreed upon by both Contractor and Company, at Contractor’s expense, to test the product for vulnerabilities through a detailed security test 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 perform an annual security test of Information Security controls which support the product, its production hosting environment, and operational support infrastructure. Contractor shall require such third party to provide a report detailing the results of the test and Contractor shall provide Company a copy of such report within thirty (30) days of the test. In the event such report shows vulnerabilities in the product, Contractor shall promptly provide Company with a proposed remediation plan and timeline for completion all at no cost to Company. All product vulnerabilities, defects, or bugs disclosed to Contractor shall be corrected and remediated by Contractor, at Contractor’s expense, within thirty (30) days from the date of such report.

1. **Right to Report**

Notwithstanding anything to the contrary in the Agreement, 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 ninety (90) days of discovery, or as agreed upon by both parties. Nothing contained in these IS Requirements shall be construed to limit any of Contractor’s other obligations regarding nondisclosure or information protection described in this Agreement.

1. **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.

1. **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.

1. **Conflicts**

Nothing contained herein shall be construed to limit any of Contractor’s obligations regarding nondisclosure or information protection contained elsewhere in this Agreement, including, without limitation, in the terms and conditions contained in the main body hereof.