**Schedule A2**

**Information security**

**requirements**

**Schedule A2**

**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 reserves the right to validate the effectiveness of the IS Requirements or Contractor shall provide evidence of 3rd party independent validation. Company shall be permitted to amend the IS Requirements upon written notification to Contractor.

# **Access Controls**

Contractor will provide role-based access, authorization, and accountability controls within their product(s) or systems(s) that process, transit or store Confidential Information and/or Confidential Customer Information (“Product” or “System”) 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 or System(s) 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 or System(s) 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 or System(s) production environment will utilize two-factor authentication when providing remote administrative support for the environment.

# Shared Architecture

Contractor agrees to 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.

# Incident Response and Breach Notification

Contractor agrees that any breach or any other security incident, internal or external that has the potential to compromise multiple data sources must be reported to the Sempra Energy Security Operations Center ([SOC@sempra.com](mailto:SOC@sempra.com) (858) 613-3278) within 24 hours of knowledge of the breach followed by a 72 hour remediation time frame, and 2 business weeks from the initial notification for completion of the investigation.

# 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) or System(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 or System(s) uses encryption keys, Contractor’s Product or System(s) will not store hard-coded encryption keys within source code. Encryption keys will be stored and secured separately from the Product or System(s) while in transit and while at rest and will be revocable for re-implementation and maintenance.

# Password and Logon Standards

Contractor’s Product(s) or System(s) will provide a unique ID (individually identifiable) for user accounts. Where individual accountability cannot be achieved for access to sensitive systems, multi-factor authentication must be employed. Contractor’s Product(s) or System(s) will provide for password complexity which conforms with the following parameters: minimum 8 characters, alphanumeric characters, 90 days password aging, and 10 previous passwords history. Logon credentials and passwords will be protected by transport encryption that meets the minimum encryption requirements of Section 4.0.

# Data Security

Contractor certifies that their Product(s) or System(s) 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.

# 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(s) or System(s), and will retain all information for a minimum of ninety (90) days from the log date. Contractor further agrees that the Product(s) or System(s) 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.

# 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) or System(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 or System(s) from being easily susceptible to cross-site scripting, SQL injection, buffer overflows, input validation, and other similar attacks. Contractor further warrants that the Product or System(s) shall not contain any code that may facilitate unexpected or unapproved access or outages to the Product or System(s), 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 Company and at no cost to Company.

# 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 or System(s), 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 or System(s), Contractor shall promptly provide Company with a proposed remediation plan and timeline for completion all at no cost to Company. All Product or System(s) 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.

# Right to Report

Company and Contractor have the right to report to public vulnerability reporting organizations regarding any defects or configuration conditions which result in vulnerabilities to information handled by the deliverable, the deliverable itself, or other hardware, software or systems that would put Company or Company’s interests at risk.

# 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.

# Formal Documentation

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

# 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.