EXHIBIT DATA-1

DATA PROTECTION AND CYBERSECURITY

This Exhibit is part of the Contract between the supplier, contractor, or consultant ("**Supplier**") and PG&E. This Exhibit applies where Supplier is accessing PG&E Systems or Processing PG&E Data, or Personal Information on behalf of PG&E. Capitalized terms not defined shall have the meanings given to them under the Contract General Terms.

I. DEFINITIONS FOR PURPOSES OF THIS EXHIBIT.

a. Personnel: any Supplier contractors, employees, or agents employed to perform Work on behalf of Supplier and that receive access to PG&E Systems or PG&E Data.

b. PG&E Data: constitutes a subset of PG&E's Confidential Information which includes:

(i) all non-public data or information provided by or on behalf of PG&E, including Personal Information;
(ii) all non-public data or information input, transferred, uploaded, migrated, or sent by or on PG&E's behalf;
(iii) all non-public data collected or received directly from PG&E, Supplier, Customers or a third party for the purposes of the Contract;
(iv) any data derived from the described in (i) through (iii), including data aggregations, summaries, analyses and reports, in each case whether de-identified or anonymized.

c. PG&E Systems: all PG&E file computing systems, databases, servers, websites, applications or network locations or domains, including, without limitation, all development, quality assurance, staging and production environments.

d. Process: means any handling or processing which is performed on PG&E Data or Personal Information, including collecting using, storing, accessing, sharing, modifying, transmitting, or deleting it.

e. Subcontractor: means a third-party individual or entity Supplier engages to perform Work on behalf of Supplier.

II. SUPPLIER PERSONNEL AND SUBCONTRACTOR REQUIREMENTS. Before providing PG&E Data to Supplier's Personnel or Subcontractor, Supplier will ensure the individual is under a legal, contractual, or other obligation that requires them to protect the PG&E Data confidentiality and security as specified in this Contract. In addition, and prior to Supplier providing PG&E Data to its Subcontractor, Supplier shall execute a written agreement with the Subcontractor that contains terms and conditions at least as restrictive as the requirements imposed on the Supplier under this Contract, and particularly this Exhibit. Supplier will give PG&E sufficient notice before engaging such Subcontractor to perform Work to allow PG&E a reasonable opportunity to object to the Subcontractor receiving PG&E Data. Supplier shall remain liable for its Personnel and Subcontractor's Work performance and compliance with the Contract requirements to protect PG&E Data and PG&E Systems.

III. USE OF PG&E SYSTEMS AND PG&E DATA. PG&E Systems and PG&E Data: (a) are and will remain confidential property of PG&E; and (b) will not be used by Supplier and its Subcontractors for any other purpose than to Process PG&E Data or access PG&E Systems reasonably necessary and proportionate to perform Work to achieve the specific business purpose for which the PG&E Data is provided. Supplier's use shall not introduce, install, or permit any Malicious Code or programs (e.g. viruses, worms, e-mail bombs, trojans) into PG&E Systems or PG&E Data.

IV. DATA RETENTION AND DESTRUCTION. PG&E Data will only be retained by Supplier for the minimum period necessary to meet Supplier's obligations under this Contract. Upon termination or expiration of the Contract, or at PG&E's request and option, Supplier will destroy or return all PG&E Data in Supplier's possession, custody, and control. When destroying PG&E Data, Supplier must follow secure industry-standard destruction practices or methods expressly approved by PG&E based on Supplier's TSR that completely remove the data so it cannot be recovered. In the case of destruction, at the written request of PG&E, Supplier will send a written confirmation of destruction.

V. DATA PROCESSING RESTRICTIONS. Unless otherwise provided in the Contract or permitted under Applicable Law,

a. Supplier shall not retain, Process, or store PG&E Data for any purpose other than performing Work; and
b. Supplier shall not sell or share (as those terms are defined in the CCPA) PG&E Data; and
c. Supplier shall not combine PG&E Data with other Personal Information Supplier receives from or on behalf of another person or collects from its own interaction with consumers.

Consumer Requests. Supplier will promptly notify PG&E if it receives a request from any person made under any Applicable Law that relates to any of the Personal Information Processed by Supplier in performing the Work (a "**Consumer Request**"). Unless otherwise required by Applicable Law, Supplier will not respond to a Consumer Request absent receiving and complying with PG&E's written instructions. Supplier agrees to assist PG&E with any Consumer Requests.

Cooperation with Audits and Risk Assessments. Upon PG&E's request and in accordance with Applicable Law, Supplier will provide reasonable cooperation and not misrepresent any fact in connection with assisting PG&E's obligations to perform a cybersecurity audit, or risk assessment involving PG&E's Data in Supplier's possession, control, or custody.

Inability to Comply. If Supplier determines it can no longer meet the obligations set forth in this Exhibit, Supplier will immediately notify PG&E in writing. Upon such notice, or upon discovery by PG&E of any non-compliance by Supplier with this Exhibit, PG&E may take reasonable steps to stop or remediate Supplier's noncompliance, including termination of the Contract, at no cost or penalty to PG&E.

Supplier Certification. Supplier certifies that it understands the obligations and restrictions imposed in this Exhibit and agrees to comply with Applicable Law related to its provision when Processing Personal Information required to do Work.

VI. SECURITY MEASURES: Supplier will implement and maintain reasonable "Security Measures" that meet or exceed industry standard cybersecurity frameworks, that at a minimum shall include:

a. Timely software, system, and equipment security updates to prevent vulnerabilities.

b. Written information security, disaster recovery, third-party assurance auditing, and penetration testing standards.

c. Premise password protections where Work is performed with access to PG&E Data hosted by Supplier or hosted on Supplier's system.

d. Encryption of any PG&E Data in transit and at rest in compliance with AES-256 or equivalent encryption standard.

e. Two-factor authentication to access PG&E Systems hosted by Supplier or PG&E Data on Supplier's system.

f. Implement commercially reasonable physical safeguards to facilities, equipment, workstations with access to PG&E Systems hosted by Supplier or with equipment that hosts PG&E Data and maintained by Supplier.

All PG&E Data must remain and only be Processed in the United States. PG&E may in its sole discretion approve in writing offshore support arrangements on a case-by-case basis.

VII. SECURITY CONTROL REVIEWS AND SECURITY BREACH: Before Supplier receives access to PG&E Systems or PG&E Data, Supplier must undergo a PG&E Third Party Security Review (TSR). If Supplier's TSR evaluation reveals or PG&E identifies any material facility, system, control, or security vulnerabilities or deficiencies, PG&E reserves the right to not provide Supplier access to PG&E Systems or PG&E Data, until such vulnerabilities or deficiencies are remedied to PG&E's satisfaction. If Supplier is unable to satisfactorily complete the TSR, PG&E shall have the right to terminate or suspend Supplier's performance of Work, access to PG&E Data or PG&E systems, at no cost or penalty to PG&E. The Supplier agrees to immediately notify PG&E in writing of any degradation in Supplier's Security Measures determined by the TSR. PG&E reserves the right to conduct periodic TSR assessments of Suppliers to ensure compliance with this Exhibit and Applicable Law.

VIII. SECURITY BREACH: Supplier will within eight (8) hours of discovery notify PG&E in writing of any actual or reasonably suspected unauthorized access to, interception, control, or acquisition of PG&E Data in Supplier's possession, custody, or control (a "Security Breach").

a. Supplier will take reasonable and remedial measures and steps to immediately stop the Security Breach and prevent recurrence.
b. Supplier will provide PG&E with reasonable information requested by PG&E in connection with any investigation of a Security Breach including but not limited to: (i) identification of the persons impacted; (ii) itemization of the documents or data impacted; (iii) status of Supplier's investigation including a summary of the Security Breach and (iv) the remedial measures that are being taken by Supplier.
c. Supplier will assist PG&E (at Supplier's sole cost and expense) in recovering or recreating any lost or inaccessible PG&E Data. Without limiting PG&E's rights under the Contract, unless the Security Breach is caused by PG&E: (i) Supplier shall be responsible for ransomware payments made to recover PG&E Data.
d. Supplier will, at PG&E's request and instructions, at Supplier's cost, notify any affected persons or entities of the Security Breach; provided that the method and content of such notice shall be agreed to in writing by PG&E prior to sending such notice. Supplier shall also cooperate with PG&E and any relevant authority in the event of litigation or regulatory inquiry concerning a Security Breach. Supplier will provide, at its sole cost, identity monitoring services for potentially affected person(s) for at least two (2) years.
e. In no event will Supplier issue or permit to be issued any public statements about the PG&E Data Security Breach that identifies PG&E, or could reasonably be associated with PG&E, unless expressly authorized by PG&E.

VIIII. RIGHT TO SEEK INJUNCTION: Supplier acknowledges that its breach of the confidentiality and data security terms of the Contract terms, including this Exhibit, may result in irreparable harm and significant injury to PG&E for which PG&E may have no adequate remedy at law. Supplier agrees that PG&E shall have the right to seek immediate temporary or preliminary injunctive relief in connection with a breach by Supplier of its confidentiality and data security terms.

IX. SUBPOENAS: If Supplier receives an order, subpoena or other legal obligation requiring disclosure of PG&E Data, Supplier will within twenty-four (24) hours of receipt, notify PG&E in writing of the request. To the extent permitted by Applicable Law, Supplier will not produce the PG&E Data until PG&E confirms in writing that it (i) was unsuccessful at quashing the requested disclosure or (ii) will not oppose the disclosure.

X. ASSISTANCE WITH REGULATORS. Upon notice to Supplier, Supplier shall assist and support PG&E in the event of an investigation by any regulator, including a data protection regulator, or similar authority, if and to the extent that such investigation relates to PG&E Data handled by Supplier on behalf of PG&E. Such assistance shall be at PG&E's sole expense, except where such investigation was required due to Supplier's acts or omissions, in which case such assistance shall be at Supplier's sole expense. Supplier shall take any other steps reasonably requested by PG&E to assist PG&E in complying with any notification, registration or other obligations applicable to PG&E under Applicable Law with respect to Personal Information. In the event this Exhibit, or any actions to be taken or contemplated to be taken in the performance of this Contract, do not or would not satisfy either Party's obligations under such laws, the Parties shall negotiate in good faith an appropriate amendment to this Exhibit.