EXHIBIT DATA-1

DATA PROTECTION AND CYBERSECURITY

This Exhibit DATA-1 forms part of the contract between the supplier, service provider, contractor or consultant ("**Supplier**") and Pacific Gas and Electric Company ("**PG&E**") to which this Exhibit DATA-1 is attached (the "**Contract**").

The term "**Services**" as used herein means any Services or Work (as applicable) to be performed by Supplier pursuant to the Contract.

1. In addition to any confidentiality or data security requirements in the Contract, Supplier shall comply with the following additional terms of this Exhibit DATA-1 regarding the protection of PG&E systems and PG&E Data (as defined below).

2. EMPLOYEE NDAs:
    a. For the purposes of this Exhibit DATA-1, "Personnel" means any Supplier personnel (including, for clarity, employees and individual contractors) and any personnel of Supplier's subcontractors who have access to PG&E systems or any Supplier systems that are used to process or store PG&E Data.
    b. Supplier shall ensure that its Personnel are under a legal obligation to protect the confidentiality of PG&E Data, and to assign intellectual property rights that they might have in Deliverables and Work Product (if applicable) to PG&E, consistent with the terms of the Contract. Supplier is not required to have an individual execute an Employee NDA as described in paragraph (c) if that individual is under a legal obligation as described in the previous sentence.
    c. For any Personnel who do not satisfy the requirements of paragraph (b), Supplier shall require each such person to sign an agreement in the form provided at the end of this Exhibit DATA-1 (an "**Employee NDA**"). Supplier shall furnish the signed Employee NDAs to PG&E (either in paper or electronic form) before the Personnel are given access to PG&E systems or PG&E Data.
    d. For the avoidance of doubt, Supplier is liable to PG&E for any failure of its Personnel to comply with the terms of this Exhibit DATA-1 or their personal confidentiality obligations with respect to PG&E Data (including, if applicable, their Employee NDA).

3. SECURITY MEASURES: Supplier shall take "Security Measures" with respect to the processing, storage and handling of PG&E Data to ensure that the PG&E Data will not be compromised, is kept secure and is used only for authorized purposes.
    a. "Security Measures" shall include at a minimum:
        i. Routine and timely security updates to devices, software and systems used to perform Services and/or to transmit, process or store PG&E Data.
        ii. Written policies regarding information security, disaster recovery, third-party assurance auditing, and penetration testing.
        iii. Password protected workstations at Supplier's premises, any premises where Services are being performed and any premises of any person who has access to PG&E Data.
        iv. Encryption of Data in transit and at rest in compliance at a minimum with AES-256.
        v. Two-factor authentication for access to any PG&E systems (including PG&E systems hosted by Supplier) or PG&E Data.
        vi. Data deletion and media sanitization processes that are compliant with NIST 800-88 and applicable PG&E policies (as disclosed to Supplier via the TSR process).
        vii. Measures to safeguard against the unauthorized access, destruction, use, control, alteration or disclosure of PG&E Data including, but not limited to, restriction of physical access to such data and information, implementation of logical access controls, sanitization or destruction of media, including hard drives, and establishment of an information security program that at all times is in alignment with the best practices described in ISO 27001 or SOC2 Type 2 as updated and replaced during the term of the Contract.
    b. All PG&E Data must remain within the United States and may only be accessed, processed and stored at locations in the United States. However, on a case by case basis (through the TSR review process) PG&E may approve offshore support arrangements that do not involve access to personal information or other sensitive information.
    c. Supplier shall update its Security Measures so as to keep current with changes in industry standards, including but not limited to ISO 2700x, SOC2, and also NIST, NERC/CIP and FERC requirements as applicable to the Services performed and types of PG&E Data that are handled by Supplier.
    d. Supplier agrees to impose on its subcontractors the same security obligations imposed on Supplier under the Contract.

4. PG&E DATA: As used herein, "**PG&E Data**" shall mean:
    a. all data or information provided by or on behalf of PG&E, including but not limited to, personal information relating to, of, or concerning, or provided by or on behalf of any Customers;

b. all data or information input, transferred, uploaded, migrated, or otherwise sent by or on behalf of PG&E to Supplier as PG&E may approve of in advance and in writing (in each instance);

c. all data collected or received by Supplier directly from any PG&E employee, agent, customer or other third party for the purposes of the Contract;

d. account numbers, forecasts, and other similar information disclosed to or otherwise made available to Supplier by or on behalf of PG&E and Customers; and

e. any data derived from the data described in paragraphs (a) through (d), including data aggregations, summaries, analyses and reports, in each case whether or not de-identified or anonymized.

5. PERIODIC SECURITY REVIEWS:

a. Annual Internal Controls Reports. Supplier shall complete an annual security audit and produce an Internal Controls Report no less frequently than annually. Supplier shall provide a copy of its most recent Internal Controls Report(s) for Supplier and its Subcontractors upon request throughout the Term. "Internal Controls Report" means a SOC 2 Type II audit report (or an equivalent independent security review report such as ISO27001 certification, including ISO27002 content, that is acceptable to PG&E) completed by an independent auditor and that covers the processes, systems and facilities used to perform the Services and/or to process or store PG&E Data. If an Internal Controls Report reveals vulnerabilities in Supplier's facilities, systems or controls, Supplier shall promptly correct such vulnerabilities.

b. PG&E's Vendor Security Review/TSR:

i. Before receiving any PG&E Data, Supplier shall undergo PG&E's Vendor Security Review (also referred to as "Third Party Security Review" or "TSR") process. This process involves responding to security questionnaires, provision of supporting information (such as existing ISO or SOC2 reports) and may also involve physical inspections of Supplier's facilities by PG&E or its designated security auditors. Supplier may receive PG&E Data if the security review reveals no high-risk security control deficiencies. If Supplier security review reveals high-risk security control deficiencies, Supplier may not receive PG&E Data until such time Supplier mitigates the risk(s).

ii. Upon request by PG&E, which will not occur more frequently than annually, Supplier shall complete an update of the Vendor Security Review process and provide such supporting information as PG&E may request to satisfy PG&E that Supplier's Security Measures are in place and are appropriate to protect PG&E Data and the systems used to process it. This updated assessment may include physical inspections of Supplier's facilities. If any such assessment reveals vulnerabilities in Supplier's facilities, systems or controls, Supplier shall promptly correct such vulnerabilities.

iii. Supplier represents and warrants that (i) statements made by Supplier in response to PG&E' security questionnaires and reviews will be true and complete, and not misleading; and (ii) Supplier will notify PG&E in writing if there is any subsequent degradation in the implemented Security Measures compared to the Security Measures that are described in its Vendor Security Review/TSR response.

c. Suspension or Termination. PG&E may terminate or suspend Supplier's performance of Services and/or Supplier's access to PG&E Data or PG&E systems, without liability to Supplier, if Supplier fails to comply with the requirements of this Section.

6. USE OF PG&E DATA:

a. License: PG&E may provide PG&E Data to Supplier to perform its obligations under the Contract. Subject to the terms of the Contract, PG&E grants Supplier a personal, non-exclusive, non-assignable, non-transferable limited license to use the PG&E Data solely for the limited purpose of performing the Services during the Contract term, but not otherwise.

b. Limited Use of PG&E Data: Supplier agrees that PG&E Data will not be (a) used by Supplier for any purpose other than that of performing Supplier's obligations under the Contract, (b) disclosed, sold, assigned, leased or otherwise disposed of or made available to third parties by Supplier, (c) commercially exploited by or on behalf of Supplier, nor (d) provided or made available to any other party without written authorization of PG&E.

c. PG&E Data shall remain the confidential property of PG&E and shall be destroyed if and when directed by PG&E. A proof of destruction should be provided to PG&E or an officer of Supplier certifies the destruction in writing to PG&E.

7. REQUIREMENTS SPECIFIC TO CALIFORNIA PRIVACY LAWS. Supplier shall comply with California privacy laws that are applicable to Supplier's performance of the Services and the handling of PG&E Data including, without limitation, the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA) as amended, updated, supplemented and replaced from time to time ("**California Privacy Laws**"). Without limiting the foregoing obligation:

a. Supplier represents and warrants that any personal information that Supplier acquires in the course of performing Services from parties other than PG&E has been and will be acquired in compliance with California Privacy Laws, including compliance with any consumer consent requirements and any consumer requests with respect to the data relating to them.

b. Supplier agrees that, except to the extent specifically required to perform Services for PG&E:

i. Supplier will not sell or share personal information (as defined in California Privacy Laws);

ii. Supplier will not retain, use, share, process, make available, disclose, or store personal information outside the direct business relationship between Supplier and PG&E, or for any commercial purpose other than as necessary to perform Services for PG&E or as otherwise permitted by California Privacy Laws;

iii. Supplier will not combine any personal information with other identifiable personal information or data that Supplier receives from or on behalf of another person or persons, or collects from its own interaction with consumers, provided Supplier may combine personal information to perform any business purpose as defined under regulations adopted pursuant to the California Privacy Laws;

c. Consumer Requests. Supplier shall promptly notify PG&E if it receives a request from an individual that relates to personal information included in PG&E Data pursuant to California Privacy Laws (a "**Consumer Request**"). Supplier shall not respond to Consumer Request(s) without written instructions from PG&E, or unless otherwise required by applicable law. Supplier shall assist PG&E with all such Consumer Requests.

d. Notification of Inability to Comply. Supplier shall immediately notify PG&E in writing if Supplier makes the determination that it can no longer meet the requirements of this Contract relating to personal information. In the event of such notification, PG&E may take reasonable and appropriate steps to stop and remediate the situation giving rise to the noncompliance, including without limitation by terminating the Contract. Such actions by PG&E shall be without prejudice to PG&E's right to claim damages with respect to Supplier's failure to perform its obligations pursuant to the Contract.

e. Supplier Certification. Supplier certifies that Supplier understands the obligations and restrictions imposed in this Contract with respect to Supplier's handling of personal information.

f. Supplier's Representation. Supplier represents and warrants that it understands and will comply with the foregoing obligations and restrictions, and that Supplier has no intent or reason to believe it will violate them.

8. SECURITY BREACH: Supplier shall immediately notify PG&E in writing of any unauthorized access to, interception or, control of or acquisition of (i) PG&E Data that is within Supplier's possession or control or (ii) Supplier's computing environment that is used to process or host PG&E Data (a "Security Breach").

   a. Supplier shall take reasonable measures within its control to immediately stop the unauthorized access or disclosure of PG&E Data, to prevent recurrence and to return to PG&E any copies.

   b. Supplier shall provide PG&E (i) a brief summary of the issue, facts and status of Supplier's investigation; (ii) the potential number of individuals affected by the Security Breach; (iii) an itemized list of the PG&E Data that is or may be implicated by the Security Breach; and (iv) any other information pertinent to PG&E's understanding of the Security Breach and the exposure or potential exposure of PG&E Data.

   c. Supplier shall 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, and shall reimburse PG&E, for any ransomware payments made in order to recover PG&E Data that is the subject of a ransomware attack; and (ii) if the Security Breach involves personal information, Supplier agrees to provide, at Supplier's sole cost and expense, appropriate identity monitoring services for all potentially affected persons for at least one (1) year following the Security Breach, subject to PG&E's prior approval; and (iii) if requested in advance and in writing by PG&E, Supplier will notify the potentially affected persons within a reasonable time period determined by PG&E and in a form as specifically approved in writing by PG&E. In addition, in no event shall Supplier issue or permit to be issued any public statements regarding the Security Breach involving PG&E Data in a manner that identifies PG&E, or could reasonably be associated with PG&E, unless expressly requested by PG&E.

9. RIGHT TO SEEK INJUNCTION: Supplier agrees that any breach of this Exhibit DATA-1 would constitute irreparable harm and significant injury to PG&E for which there is no adequate remedy at law and that it will not be possible to measure precisely damages for such harm. Accordingly, and in addition to PG&E's right to seek damages and any other available remedies at law or in equity in accordance with the Contract, Supplier agrees that PG&E will have the right to obtain, from any competent civil court, immediate temporary or preliminary injunctive relief enjoining any breach or threatened breach of the terms of this Exhibit DATA-1, involving the alleged unauthorized access, disclosure or use of PG&E Data. Supplier hereby waives any and all objections to the right of such court to grant such relief, including, but not limited to, objections of improper jurisdiction or forum non conveniens.

10. SUBPOENAS: In the event that a court or other governmental authority of competent jurisdiction, including the CPUC, issues an order, subpoena or other lawful process requiring the disclosure by Supplier of PG&E Data, Supplier shall notify PG&E immediately upon receipt thereof to facilitate PG&E's efforts to prevent such disclosure, or otherwise preserve the proprietary or confidential nature of the PG&E Data. If PG&E is unsuccessful at preventing the disclosure or otherwise preserving the proprietary or confidential nature of the PG&E Data, or has notified Supplier in writing that it will take no action in that regard, then Supplier shall not be in violation of this Contract for its compliance with the court order or governmental authority with respect to such disclosure.

Exhibit DATA-1 (rev February 2023)

EMPLOYEE NDA

This Agreement is between the individual who signs the Contract in the signature block below ("**Employee**") and Pacific Gas and Electric Company ("**PG&E**").
Employee works for the company identified below (the "**Supplier**") as an employee, independent contractor or subcontractor. Supplier has been engaged directly by PG&E or as a subcontractor to provide services to PG&E ("**Services**"). Supplier wishes to utilize Employee to perform some of those Services. In consideration for PG&E giving Employee access to PG&E's systems and information, Employee acknowledges and agrees to the following.

1. **Confidentiality.** Employee will keep all PG&E Data (as defined below) strictly confidential, and will not copy, disclose or use it for any purpose other than as necessary to perform Services for PG&E and in accordance with directions given to Employee by the Supplier. PG&E Data is PG&E's sole property.
2. **Background Checks**. Employee acknowledges that PG&E may conduct background checks on Employee before granting Employee access, and may deny Employee access based on the results of those checks. Employee consents to such checks.
3. **Security.** Employee will follow all directions given to Employee by the Supplier regarding the proper and secure access to, and use of, PG&E systems and assets. Employee will access and use those systems and assets only to perform Employee's assigned duties for PG&E. The Supplier will give Employee copies of PG&E's standards and policies governing access to and use of PG&E computer systems and resources. Employee will comply with them. In particular, Employee will use any user ID, password and Access Cards that are furnished to Employee only for Employee's own use in performing Services for PG&E. Employee will keep them confidential and will not share them with others.
4. **Not a PG&E Employee.** Employee acknowledges and affirms that he or she remains an employee, independent contractor or subcontractor of the Supplier and nothing in the Contract changes Employee's status or makes Employee an employee of PG&E. Employee will continue to take direction from, and will be supervised by, the Supplier in Employee's work for PG&E.
5. In the Contract:
   "**PG&E Data**" means: (i) any computer resources, technical information and materials contained in or relating to PG&E systems that Employee may view, access or receive in the course of performing Services for PG&E including but not limited to: computer systems, electronic records processed and/or stored in such systems, specifications and records and/or software, data, computer models, and related documentation; and (ii) any data stored in or obtained from PG&E systems; and (iii) any changes or updates to any of the foregoing that Employee may make in the course of performing Services for PG&E.
6. **Notice of Immunity**: Federal law provides that an individual shall not be held criminally or civilly liable under any Federal or State trade secret law for the disclosure of a trade secret that—
   (A) is made—
   (i) in confidence to a Federal, State, or local government official, either directly or indirectly, or to an attorney; and
   (ii) solely for the purpose of reporting or investigating a suspected violation of law; or
   (B) is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal.
   In addition, an individual who files a lawsuit for retaliation by an employer for reporting a suspected violation of law may disclose the trade secret to the attorney of the individual and use the trade secret information in the court proceeding, if the individual—
   (A) files any document containing the trade secret under seal; and
   (B) does not disclose the trade secret, except pursuant to court order.

Employee confirms his or her agreement with these terms by signing and dating this document below:

_____
Name of Employee

_____
Signature

_____
Title/Position

_____
Date

_____
Name of Supplier