MUTUAL NONDISCLOSURE AGREEMENT

This MUTUAL NONDISCLOSURE AGREEMENT ("**NDA**"), by and between Pacific Gas and Electric Company, a California corporation ("**PG&E**"), and County of Tehama a political subdivision of the State of California ("**Company**") (together the "**Parties**" and each individually a "**Party**"), is effective as of the latest signature date below (the "**Effective Date**").

WHEREAS, PG&E is an investor-owned utility that provides gas and electric service to millions of customers throughout Northern and Central California;

WHEREAS, County of Tehama is a political subdivision of the State of California headquartered in Red Bluff, Tehama County, California, and is exploring the development of a microgrid, developing a microgrid, or has developed and is maintaining a community microgrid pursuant to PG&E's Community Microgrid Enablement Tariff ("**CMET"**);

WHEREAS, in support of those efforts, the Parties expect that each Party may disclose to and receive from the other Party some amount of Confidential Information, as defined herein;

WHEREAS, the Parties recognize that the development of microgrids is in the public's interest; and

WHEREAS, each Party wishes to protect, use, handle, and safeguard the Confidential Information that it receives from the other Party in compliance with law and in accordance with the duties and responsibilities set forth herein.

NOW THEREFORE, the parties agree as follows:

1. **Purpose**. The purpose of this Agreement is to permit each Party to transmit or exchange Confidential Information to or with the other Party hereto for the purpose of evaluating and reviewing such Information in connection with the potential or actual development, operation and maintenance of a microgrid pursuant to PG&E's CMET ("Purpose"), and for no other purpose. The Parties mutually agree that development of microgrids is in the public's interest and that the Purpose of this Agreement justifies maintaining the confidentiality of their respective Confidential Information.

2. **Confidential Information.** "**Confidential Information**" as used herein shall mean any non-public proprietary or confidential data, information and other materials including those regarding the products, services or business of the disclosing party (the "**Disclosing Party**"), its parent company, its subsidiaries or affiliates (and/or if either Party is bound to protect the confidentiality of any third party, of such third party) provided by or made available by the Disclosing Party to the receiving party (the "**Receiving Party**") where such information is marked or otherwise communicated as being "proprietary" or "confidential" or the like. Without limiting the foregoing, Confidential Information includes (i) all confidential and proprietary documents, records, reports, agreements and associated documents; (ii) any and all information pertaining to PG&E's electric distribution and transmission facilities; (iii) all technical, financial and business information of any kind; (iv) all written procedures; (v) all data, specifications, technology, ideas, know-how, improvements, maps, technical drawings, inventions (whether or not patentable or copyrightable), or trade secrets; and (vi) all Personal

Information belonging to the Disclosing Party. Confidential Information does not include information which: (a) is already known to the Receiving Party on a non-confidential basis prior to the disclosure by Disclosing Party; (b) becomes publicly available without breach of the confidentiality obligations of this NDA by Receiving Party or its representatives; (c) is approved for release without confidentiality obligations by written authorization of the Disclosing Party; (d) is rightfully obtained by Receiving Party from a third party without restriction as to disclosure; (e) is developed independently by Receiving Party without use of or access to Disclosing Party's Confidential Information.

[For public entity counterparties: Furthermore, and consistent with the Purpose of the Agreement, the Parties agree that they are sharing Confidential Information to serve the public's interest and that this Purpose clearly outweighs publicly disclosing such Confidential Information. Accordingly, the Parties agree that Disclosing Party's Confidential Information is exempt from disclosure pursuant to the California Public Records Act, California Government Code § 6250, et seq., and other federal, state, and municipal public disclosure laws, including but not limited to the Brown Act, California Government Code § 54950, et seq., and shall remain confidential as set forth in Paragraph 9 of this Agreement, entitled "Term and Termination"]

3. **Processing Personal Information.** "**Personal Information**" as used herein shall mean any information provided by PG&E, its subsidiaries, affiliates, agents, officers, directors, current and former employees, or customers, to Company that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual, or as the "personal information" or "personal data" or such similar term is defined under applicable data privacy and protection laws. In the event Personal Information related to its employees, customers or other individuals is disclosed to Company, the Parties agree that the provisions detailed in the Personal Data Processing Addendum, attached hereto as Appendix A, shall apply. In the event of any conflict with regard to Personal Information between the general terms of this Agreement and Appendix A, the terms of Appendix A will govern.

4. **Use and Nondisclosure of Confidential Information.** Receiving Party agrees to keep any Confidential Information made available or provided to it as confidential and proprietary and shall treat such Confidential Information in the same manner as it treats is own similar proprietary and confidential information, but in no case will the degree of care be less than reasonable care. The Receiving Party shall use the Confidential Information only in performing its obligations or to exercise its rights in connection with the Purpose. The Receiving Party shall not sell, share or otherwise disclose Confidential Information to any third party (except as authorized under the NDA or applicable law) without the Disclosing Party's express written consent. The Receiving Party shall disclose Confidential Information only to those employees and contractors of Receiving Party who have a need to know such information for the purposes of performing its obligations or exercising its rights in connection with the Purpose, and such employees and contractors must be bound by an NDA or have entered into agreements with Receiving Party containing confidentiality provisions covering the Confidential Information with terms and conditions at least as restrictive as

those set forth in this NDA. Unless expressly required by the Purpose, the Receiving Party shall not input or otherwise process Confidential Information using generative artificial intelligence or any similar program or algorithm except with the express, prior, written permission of the Disclosing Party.

The Parties further agree that this Agreement shall not be construed to limit either Party's right to independently develop or acquire products without use of or reference to the other Party's Confidential Information. The Disclosing Party acknowledges that the Receiving Party may currently or in the future develop information internally, or receive information from other parties, that is similar to the Confidential Information. Accordingly, nothing in this Agreement will be construed as a representation or agreement that the Receiving Party will not develop or have developed products, concepts, systems, or techniques that are similar to or compete with the products, concepts, systems or techniques contemplated by or embodied in the Confidential Information provided that the Receiving Party does not violate any of its obligations under this Agreement in connection with such development.

5. **Security Measures**. The Receiving Party shall implement reasonable administrative, technical and physical security measures to safeguard the Confidential Information it receives. These safeguards shall include, but not be limited to: (a) written policies regarding information security, disaster recovery, third-party assurance auditing, penetration testing; (b) password protected workstations at Receiving Party's premises, any premises where services are being performed and any premises of any person who has access to such Confidential Information, and (c) encryption of Confidential Information.

6. **Disclosures Required by Law**. If any Confidential Information is required to be disclosed by law, rule, regulation, court of competent jurisdiction or governmental order, then to the extent permitted by applicable law, the Receiving Party shall advise the Disclosing Party of the Confidential Information required to be disclosed promptly upon learning thereof in order to afford the Disclosing Party (at the Disclosing Party's sole cost and expense) a reasonable opportunity to contest, limit or assist the Receiving Party in crafting the disclosure, and then such disclosure shall be made only to the extent necessary to satisfy such requirements. Notwithstanding the foregoing, the Parties recognize that PG&E is a regulated utility and that its regulators have broad rights to request information from PG&E and from time-to-time PG&E may have to disclose certain Confidential Information to its regulators (e.g., the California Public Utilities Commission (CPUC) and the Federal Energy Regulatory Commission (FERC)). In that event, PG&E will disclose such information subject to the regulators' respective confidentiality rules.

7. **Unauthorized Disclosures**. The Receiving Party shall promptly notify the Disclosing Party in writing of any unauthorized access or disclosure of Confidential Information. The Receiving Party shall take reasonable measures within its control to stop the unauthorized access or disclosure of Confidential Information and to prevent recurrence. The Parties agree that a breach of this NDA would constitute irreparable harm and significant injury to the Disclosing Party. The Disclosing Party therefore shall have the right to seek from any competent civil court, immediate temporary or preliminary injunctive relief enjoining any breach or threatened breach of this NDA.

8. **Return or Destruction of Confidential Information.** All Confidential Information disclosed by Disclosing Party to Receiving Party remains the property of the Disclosing Party, and Receiving Party shall return or destroy all Confidential Information, including any copies of Confidential Information in its or its agents' possession upon the termination of this NDA or otherwise at the Disclosing Party's request. Within fifteen (15) days of receiving such request from the Disclosing Party, the Receiving Party shall comply with the request and provide written certification, signed by the Receiving Party, confirming the Receiving Party's compliance with the return or destruction of all Confidential Information as set forth in this provision. Notwithstanding the foregoing, the Receiving Party may retain one copy of Confidential Information for purposes of complying with its legal obligations or consistent with Receiving Party's backup retention and recovery purposes, provided that the obligations set forth in this NDA apply to any retained Confidential Information.

9. **Term and Termination.** This NDA shall be effective from the Effective Date, provided however, that either Party may terminate this NDA by giving the other Party thirty (30) calendar days' notice in writing of its intention to terminate this NDA. Termination shall not abrogate either Party's obligations under this NDA for Confidential Information received prior to the date of termination.

10. **Notices.** Any notice required to be sent or given under this Agreement will be sent via electronic mail, addressed as follows:

PG&E	County of Tehama
Name: Andrea Schumer	Name: CAO Gabriel Hydrick
E-Mail: communitymicrogrids@pge.com	E-Mail: ghydrick@co.tehama.ca.us
Phone: (510) 697-3968	Phone: (530) 527-4655

11. **Communications and Media.** Neither Party will disclose any information or make any news release, advertisement, public communication, response to media inquiry or other public statement regarding this Agreement, the Confidential Information disclosed, the Purpose and/or potential commercial relationship between the Parties, or the performance hereunder without the prior written consent of the other Party. Subject to Paragraph 5, neither Party will make any reference to the other Party or to the existence of this Agreement in any advertising or other publication (except for confidential, internal company publications), without the prior written consent of the other Party, and neither Party will associate or in any way connect its name, trademark or any other intellectual property right to any name, trademark or any other intellectual property right of the other Party without the other Party's prior written consent. The fact that the Parties have entered into this Agreement does not constitute, nor does it imply in anyway, endorsement by one Party of the other, and neither Party will indicate or imply that the other Party endorses, recommends, or vouches for it in any form of written, verbal, or electronic advertisement, communication, or any other business development effort, without the other Party's prior written consent.

12. **No License**. No license or proprietary rights are granted by disclosure of any Confidential Information under this NDA. For avoidance of doubt, nothing in this NDA is intended to

grant any rights to any Receiving Party under any patent, copyright, trade secret or other intellectual property right nor does this NDA grant any Receiving Party any rights in or to the Confidential Information, except the limited right to use the Confidential Information solely for the Purpose.

13. **Compliance with Applicable Law**. The Receiving Party agrees to comply with all applicable laws governing the protection of the Confidential Information.

14. **Indemnification.** The Receiving Party shall indemnify the Disclosing Party against any and all actions, claims, liabilities, costs, damages, charges and expenses incurred in connection with or arising out of the Receiving Party's use of Confidential Information.

15. **Assignment.** Neither Party shall assign this NDA nor any Confidential Information received from Disclosing Party pursuant to this NDA without Disclosing Party's prior written consent. This NDA shall be binding upon each Party, their successors, and assigns.

16. **No Warranty**. All Confidential Information is provided "as is" without any warranties, express, implied, or otherwise, regarding the accuracy or completeness of any Confidential Information disclosed by the Disclosing Party to the Receiving Party.

17. **Severability and Waiver**. The covenants and agreements set forth in this NDA are each deemed separate and independent, and if any such covenant or agreement is determined by any court of competent jurisdiction or arbitrator/mediator to be invalid or unenforceable for any reason, the Parties shall negotiate an equitable adjustment in the provisions of this NDA with a view toward effectuating the purpose of this NDA. The invalidity or unenforceability of any of the provisions, or application of any of the provisions, of this NDA will not affect the validity or enforceability of any of the remaining provisions of this NDA.

18. **Entire Agreement.** This NDA contains the entire understanding between the Parties with respect to Confidential Information received hereunder. This NDA has been negotiated by both Parties and shall not be strictly construed against either Party. No change, modification, extension, termination, or waiver of this NDA shall be made effective unless in writing and signed by an authorized representative of each Party.

19. **Governing Law**. This NDA shall be construed and interpreted in accordance with the laws of the State of California. Any controversy, dispute, issue, or claim arising out of or in any way relating to this NDA which cannot be amicably settled without court action shall be litigated in a California State Court of competent jurisdiction; or if jurisdiction over the action resides in the federal courts, then in a Federal Court of competent jurisdiction situated in the State of California.

20. **Counterparts**. This NDA may be executed in one or more counterparts, each of which shall be deemed an original and all of which, when taken together, constitute one and the same instrument. The Parties agree that electronic signatures may be used for execution of the NDA. The email, PDF or other electronically delivered signatures of the Parties shall be

deemed to constitute original signatures, and electronic copies of the executed NDA shall be deemed to constitute duplicate originals.

21. **Remedies.** Notwithstanding any other term of this NDA, it is expressly agreed that a breach of this NDA will cause irreparable harm to the Disclosing Party and that a remedy at law would be inadequate. Therefore, in addition to any and all remedies available at law, the Disclosing Party will be entitled to injunctive and/or other equitable remedies in the event of any threatened or actual violation of any provisions of this NDA. In any dispute between the Parties arising out of or relating to the NDA, the prevailing party shall be entitled to recover from the opposing party his or its attorneys' fees and costs.

Signature page follows

IN WITNESS HEREOF, and intending to be legally bound hereby, the Parties hereto have caused this NDA to be executed by their duly authorized representatives as of the Effective Date.

[COMPANY] County of Tehama	**PACIFIC GAS & ELECTRIC COMPANY**
Signature:	Signature:
Name: County of Tehama	Name: Andrea Schumer
Title: CAO	Title: Principal Resilience Coordinato
Date:	Date:

Appendix A

PERSONAL DATA PROCESSING ADDENDUM

This Personal Data Processing Addendum ("**DPA**") amends, in accordance with the terms set forth below, all agreements between the Parties, pursuant to which Company receives and processes Personal Information (as defined below) and to clarify and confirm Company's obligations to safeguard and maintain the security of the Personal Information it collects from or on behalf of PG&E related to employees, dependents and beneficiaries, consultants, workers, visitors, shareholders, and/or customers of PG&E and its subsidiaries and affiliates.

1. **DEFINITIONS**. As used in this DPA, the following capitalized terms shall have the meanings provided in this section. Capitalized Terms used in this DPA, but not defined below have the meaning given to them in the Parties' Agreement.

Agreement. "Agreement" means the Mutual Non-Disclosure Agreement by and between PG&E and Company.

Personal Information. "Personal Information" means any information provided by PG&E, its subsidiaries, affiliates, agents, officers, directors, current and former employees, or customers, to Company and that identifies, relates to, describes, is reasonably capable of being associated with or could reasonably be linked, directly or indirectly, with a particular individual. "Personal Information" includes "personal information," "personal data" or other such similar terms as they are defined under applicable Privacy Laws.

Privacy Laws. "Privacy Laws" are all applicable laws, rules, regulations, directives and governmental requirements in any jurisdiction in which Company or Company operates and relating in any way to the privacy, confidentiality, or security of Personal Information processed by Company, including, but not limited to the California Consumer Privacy Act of 2018 ("CCPA") and the California Privacy Rights Act of 2020 ("CPRA").

2. **CONTROL OF PERSONAL INFORMATION**. PG&E shall retain all ownership and control over the Personal Information disclosed to Company. PG&E also has the exclusive authority to determine the purposes of processing of all Personal Information by Company.

3. **LIMITED USE OF PERSONAL INFORMATION**. At all times during the term of this DPA and thereafter, Company shall collect (including, without limitation, caching or storing), access, use, disclose, process or retain Personal Information solely for the purpose of rendering the contracted services to PG&E and not for any other purpose. Company shall not sell, share or otherwise disclose any Personal Information to any third party except as expressly permitted herein. Company shall not use any Personal Information to violate or attempt to violate the security of PG&E's systems, or any third party networks, system, server, website, application or account.

4. **ADDITIONAL RESTRICTIONS.** Company shall not: (i) sell or share Personal Information or (ii) collect, retain, use, or disclose Personal Information for any purpose other than for the specific purpose of performing the services specified in the Agreement. For avoidance of doubt, Company shall not collect, retain, use, or disclose Personal Information for any commercial purpose other than providing the services specified under the Agreement unless otherwise permitted under applicable law. For purposes of this section, the terms "sell," "commercial purposes" and "personal information" shall have the meanings as defined under the CCPA and "share" shall have the meaning as defined under the CPRA.

5. **AGENTS**. Company shall not contract any of its rights or obligations hereunder, or share, transfer, disclose or otherwise provide access to any Personal Information to any contractors, subcontractors, third-party service providers, or agents (collectively, "Agents") without the prior written consent of Company. Where Company contracts any rights or obligations, or provides access to Personal Information, to an Agent, then (a) Company shall enter into a fully-executed written agreement with each Agent that imposes obligations on the Agent that are at least as restrictive as those imposed on or required of Company under this DPA; (b) Company shall not be relieved of any of its obligations under this DPA; and (c) Company shall remain liable and responsible for the performance or non-performance of its Agents with respect to the Agent's collection, use, disclosure, storage, processing and disposal of Personal Information.

6. **COMPLIANCE WITH LAW**. Company agrees that its collection, use, disclosure, storage, processing and disposal of Personal Information shall at all times comply with all applicable Privacy Laws and any representations made by Company to any person from whom such Personal Information was collected. Company further agrees that it will reasonably cooperate with PG&E's efforts to comply with PG&E's legal obligations related to its collection, processing, use or disclosure of Personal Information.

7. **DATA SECURITY**. Company shall, and shall contractually require and cause any Agents to, implement and maintain security procedures and practices for Personal Information, including without limitation, establishing, implementing and maintaining an Information Security Program as set forth in this Section 7, that will: (i) comply with all applicable Privacy Laws and industry standards; (ii) ensure the security and confidentiality of Personal Information, (iii) protect against any anticipated or actual threats or hazards to the security or integrity of Personal Information, and (iv) prevent unauthorized access, acquisition, destruction, use, modification and/or disclosure of Personal Information. Company and its Agents shall each ensure that its security infrastructures are consistent with high industry standards for virus protection, firewalls and intrusion prevention technologies to help prevent Company's network, systems, servers and applications from unauthorized access. Company will restrict and track access to Personal Information and PG&E systems at all times to only those employees and Agents whose access is essential to performing the services for which Company has been contracted, and such employees and Agents will be required (including during the term of their employment or retention and thereafter) to protect Personal Information in accordance with the requirements of this DPA. Company shall segregate Personal Information from all other Company and third party data. Company must ensure proper user authentication for all employees, and Agents with access to Personal Information, including, without limitation, by assigning

each employee or Agent unique access credentials for access to any system on which Personal Information can be accessed and prohibiting employees and Agents from sharing such access credentials. Company shall ensure that upon termination of any employee or Agent, the terminated person's access to Personal Information and PG&E systems must be immediately revoked.

8. **INFORMATION SECURITY PROGRAM**. Company shall conduct appropriate training and awareness campaigns designed to educate Company's employees of their responsibilities in maintaining the confidentiality and security of Personal Information and for the reporting of incidents involving unauthorized access to or use of Personal Information, consistent with all Privacy Laws and the terms of this DPA. Company represents and warrants that it has implemented and will maintain a variety of administrative, organizational and technical measures ("Information Security Program) that are consistent with industry standards which may include but are not be limited to ISO 27001/2, NIST, OWASP, and other similar standards that are designed to reasonably and appropriately protect the confidentiality, integrity mid availability of information systems or data and which measures are set forth below. Company shall review its Information Security Program on at least an annual basis and evaluate whether it needs to be modified to comply with Privacy Laws or industry practices. Company shall notify PG&E of any material changes to Company's Information Security Program as it relates to the security and integrity of Personal Information, within thirty (30) days of any such change. Notwithstanding the foregoing, at all times, Company's Information Security Program shall include the following:

a. Organizational management and dedicated staff responsible for the development, implementation and maintenance of Company's Information Security Program.

b. Audit and risk assessment procedures designed for the purposes of periodic review and assessment of risks to Company's organization, for monitoring and maintaining compliance with Privacy laws, and for reporting the condition of its information security and compliance to Company senior management.

c. Data security controls which include at a minimum, but may not be limited to, logical segregation of data, restricted (e.g., role-based) access and monitoring, and utilization of commercially available and industry standard encryption, at a minimum of 256-bit encryption, for Personal Information that is:

    i. transmitted order public networks (i.e. the Internet) or when transmitted wirelessly,

    ii. stored on any Company or Agent systems, including any cloud based systems.

d. Logical access controls to manage electronic access to data and system functionality based on authority levels and job functions, *(e.g.* granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all

users, periodic review and revoking/changing access promptly when employment terminates or changes in job functions occur).

e. Password controls to manage and control password strength, expiration and usage including prohibiting users from sharing passwords.

f. System auditor event logging and related monitoring procedures to proactively record user access and system activity for routine review.

g. Physical and environmental security of data center, server room facilities and other areas containing Personal Information to protect information assets from unauthorized physical access, and to manage, monitor and log movement of persons into and out of Company facilities, and to guard against environmental hazards such as heat, fire and water damage.

h. Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems according to prescribed internal and adopted industry standards, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from Company's possession.

i. Change management procedures and tracking mechanisms to ensure all changes to Company's technology and information assets are properly tested, approved and monitored.

j. Incident management procedures to allow for the proper investigation, response, mitigation and notification of events related to Company's technology and information assets.

k. Network security controls that provide for the use of enterprise firewalls and layered DMZ architectures, and intrusion detection systems and other traffic and event correlation procedures to protect systems from intrusion and limit the scope of any successful attack.

l. Vulnerability assessment, patch management, and threat protection technologies and scheduled monitoring procedures to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.

m. Business continuity and disaster recovery procedures to ensure Company's ability to maintain service and/or recovery from foreseeable emergency situations or disasters.

n. Controls to ensure any applicable Company software is securely developed in accordance with this DPA, such as design reviews, secure separation of development and production environments, code reviews, and quality assurance testing.

9. **TRANSMISSION OF PERSONAL INFORMATION**. Company shall not electronically transmit a record containing Personal Information outside a secure network environment other than by a secure network connection or communications protected by appropriate encryption technology that is not less than 256-bits in length. Likewise, Company shall not require any individual to transmit Personal Information over the Internet unless the connection is secure or the Personal Information is protected by encryption technology meeting this standard. Company shall not print Personal Information on mailed material unless required by law and will not make Personal Information visible through any envelope window unless required by law. Notwithstanding the provisions of this Section, when strictly necessary to perform the contracted services and permitted by applicable Privacy Laws, Personal Information may be included in applications and forms sent by mail, including documents sent as part of an application or enrollment process, or to establish, amend or terminate an account, contract or policy, or to confirm the accuracy of the Personal Information.

10. **SECURITY MANAGER**. On the effective date of the Agreement, Company shall designate an individual as the primary security manager under this DPA. The security manager shall be responsible for managing and coordinating the performance of Company's privacy and data security obligations under this DPA.

11. **SUBPOENAS AND LEGAL PROCEEDINGS**. Subject to applicable law, Company shall immediately notify PG&E of any subpoena or other judicial or administrative order by a court, tribunal, litigant, or government authority seeking access to or disclosure of Personal Information. Subject to applicable law, PG&E shall have the right take steps to assess and/or prevent such disclosure and to defend subpoena enforcement proceedings or motions to compel in lieu of and on behalf of Company, which still must provide reasonable cooperation to PG&E in connection with such defense.

12. **DATA SECURITY BREACH NOTIFICATION AND INCIDENT RESPONSE**. Company shall notify PG&E, of: (a) any access, possession, use or disclosure of Personal information, or attempt thereof, not expressly permitted by this DPA; (b) any suspected breach or compromise of Personal Information, or Company's systems or networks that directly or indirectly support Personal Information; or (c) claims or threats thereof made by any personnel, Agent or external person (each or the foregoing a "Data Security Breach"). Company shall notify PG&E of a Data Security Breach within twenty-four (24) hours after detecting or being notified of the Data Security Breach affecting Personal Information.

a. **Data Security Breach Investigation**. Company shall immediately take measures to stop the Data Security Breach and in PG&E's sole discretion, upon PG&E's written request, and pursuant to PG&E's instructions, Company shall cooperate with PG&E and any outside agents hired by PG&E in connection with: (i) conducting an investigation of any actual or suspected Data Security Breach and (ii) providing PG&E and its agents with administrative access to all affected systems or applications that store, process, transmit or otherwise access Personal Information. Company shall provide PG&E with the following information, at minimum: (i) a brief summary of the issue, facts and status of Company's

investigation; (ii) the potential number of individuals affected by the Data Security Breach; (iii) the Personal Information that has been or may have been implicated by the Data Security Breach; and (iv) any other information pertinent to PG&E's understanding of the Data Security Breach and the exposure or potential exposure of Personal Information.

b. **Other Parties**. Unless the Data Security Breach impacts the information of parties other than PG&E, Company shall not notify any parties other than PG&E and relevant law enforcement agencies of any Data Security Breach unless such notification is agreed to in advance by PG&E in writing.

c. **Resolution**. For avoidance of doubt, any Data Security Breach vulnerability shall be resolved to PG&E's satisfaction, at Company's expense. If such vulnerability cannot be resolved to PG&E's satisfaction within a reasonable period of time, as determined by PG&E, PG&E shall have the right to immediately terminate the Agreement without liability.

d. **Notification.** Company will, upon PG&E's written request and pursuant to PG&E's instructions, at Company's cost, notify any affected persons or entities provided that the method and content or such notice to shall be agreed to in writing by PG&E prior to sending such notice. Company shall also cooperate with PG&E and any relevant authority in the event of litigation or regulatory inquiry concerning a Data Security Breach. Notwithstanding the foregoing, Company, at its sole expense shall investigate and remediate all Data Security Breaches.

e. **Indemnification**. In addition to Company's indemnification obligations set for in Section 21 of this DPA, Company shall also indemnify, hold harmless, and defend PG&E and its respective directors, officer; employees, subcontractors and agents from any suits, claims, damages, demands, proceedings, and other actions brought by a third party, and all associated expenses and costs (including but not limited to: assessments, fines, losses, penalties, costs of investigating and responding to any Data Security Breach, costs of notifying affected individuals, and attorneys' fees), arising out of or related to Company's or its Agents collection, processing, storage, use transmission or destruction of Personal Information, including, but not limited to, a suspected or actual Data Security Breach. The remedies set forth herein shall be in addition to any other remedies available to PG&E at law or in equity, including but not limited to Company's general indemnification obligations set forth in this DPA.

13. **CREDIT MONITORING**. In the event of a Data Security Breach (including, without limitation, by an unauthorized employee or Agent of Company), at the sole discretion of PG&E, Company will offer Credit Monitoring Services (as defined below) as designated by company to any affected individual at Company's cost and expense. Affected individuals will be notified of the availability of Credit Monitoring Services as directed by PG&E, at Company's sole cost. "Credit Monitoring Services" mean credit monitoring services for two (2) years, beginning on the date the individual first registers for the

service after the Data Security Breach or such period required by Privacy Laws and one (1) free credit report provided by Experian, Equifax, or TransUnion.

14. **DESTRUCTION AND RETURN OF PERSONAL INFORMATION**. As soon as possible after any of the Personal Information (or portion thereof) is no longer needed by Company to fulfill its obligations to PG&E or upon PG&E's written request, or in the event of termination or expiration of this DPA for any reason, Company shall, and shall cause its Agents, to immediately securely destroy and certify such secure destruction (and produce a written certification upon request by PG&E) of any or all of Personal Information and all records of Personal Information, (including, without limitation, all electronic copies such as on hard drives, backup tapes, portable devices, optical, magnetic, or other storage media, as well as all hard copies) or, if requested by PG&E, return Personal Information to PG&E through a secure method designated by PG&E. Company shall ensure that Personal Information is destroyed in accordance with the methods described in the Federal Trade Commission's Disposal Rule, 16 C.F.R § 682.3 and any other Privacy Law.

15. **SECURITY AUDIT RIGHTS**. At the request of PG&E and at PG&E's cost, Company shall provide PG&E, or an independent third-party auditor selected by PG&E, access to, and the right to conduct a security audit of, all records, security policies and procedures, and other practices relating to the use, processing, storage and disclosure of Personal Information. The audit results and Company's plan for addressing or resolving issues identified by the audit shall be shared with PG&E within ten (10) days of Company's receipt of the audit results. If Company fails to resolve the issues identified in its plan within a reasonable timeframe determined by PG&E, PG&E shall have the right to terminate the services contract between the Parties. In addition, subject to Company's advance approval as to scope and timing, PG&E also reserves the right to conduct, at its own cost, not more than twice per calendar year, technical security integrity reviews, and penetration tests and monthly Internet security scans to ensure Company remains compliant with this DPA (collectively, "Application Security Assessments"). PG&E will provide seven (7) days' notice prior to penetration testing or the commencement of monthly scanning activities. Company shall correct any security flaw discovered by PG&E within eight (8) hours. Further, Company and any Agent that accesses, stores or collects Personal Information shall conduct, at its own cost, an Application Security Assessment annually using an independent third-party tester.

16. **MALICIOUS CODE**. Company will ensure that the contracted services will not result in the transmission to PG&E of any (a) 'back door', 'time bomb', 'Trojan Horse,' 'worm', 'drop dead device,' 'virus', 'spyware' or 'malware;' or (b) any computer code or software routine that: (i) permits unauthorized access to or use of PG&E's or its users' systems or any component thereof; or (ii) disables, damages, erases, disrupts or impairs the normal operation of PG&E's or its users' systems or any component thereof.

17. **INTERNATIONAL TRANSFER OF DATA**. Company shall not transfer Personal Information to, or allow access to Personal Information by, its employees or Agents in any location outside the United States without receiving the prior written consent of PG&E. To the extent that the parties agree to the transmission of Personal Information outside of the

United States, prior to making any such transfer, the parties will negotiate in good faith and agree to the terms of a data transfer agreement that complies with applicable Privacy Laws governing the cross-border transfer of Personal Information.

18. **SUSPENSION OF DATA TRANSFERS**. PG&E reserves the right to suspend or stop data transfers to Company at any time. In the event that Company is unable to comply with the obligations stated in this DPA, Company shall within forty-eight (48) hours notify PG&E, and PG&E shall then be entitled (at its option) to suspend the transfer of Personal Information, require Company to cease using Personal Information and/or immediately terminate the Agreement PG&E may have with Company that requires the transfer of Personal Information for the contracted services.

19. **DATA SUBJECT REQUESTS**. Company shall promptly send PG&E within three (3) business days of receipt of any communication received from an individual relating to his or her request to access, modify or correct, or delete Personal Information relating to the individual or to opt-out of any program or communication and Company shall comply with instructions of PG&E before responding to such data subject requests.

20. **COOPERATION WITH GOVERNMENT ENFORCEMENT AUTHORITIES**. Company will provide reasonable cooperation to PG&E in connection with PG&E's efforts to respond to any complaint filed with, or investigation conducted by, any government agency or data protection authority resenting the processing of Personal Information by Company.

21. **INDEMNIFICATION**. Notwithstanding anything to the contrary in any agreement between PG&E and Company, Company shall indemnify, hold harmless, and defend PG&E and its any and officers, employees, subcontractors, agents, successors, and assigns from and against any and all claims, losses, liabilities, damages, settlements, expenses and costs (including without limitation attorneys' fees and court costs) and any and all threatened claims, losses, liabilities, damages, settlements, expenses and costs arising from, in connection with, or based on allegations of, in whole or in part, any of the following: (a) any violation of the requirements of this DPA; (b) any negligence or willful misconduct of Company, its personnel or Agents or any third party to whom Company provides access to Personal Information or systems, with respect to security or confidentiality of Personal is (c) any other costs incurred by PG&E with respect to PG&E's rights in this DPA. Except as otherwise provided herein, Company shall be fully responsible for, and shall pay, all costs and expenses incurred by Company or its personnel, third-party service providers of Company or Agents with respect to the obligations imposed under this DPA.

22. **RELATION TO THE AGREEMENT**. A breach of any term of this DPA will be deemed a breach of the Agreement. The provisions of the Agreement regarding the subjects of Breach, Choice of Law, and Venue shall govern the parties' respective rights and obligations under this DPA. Notwithstanding the foregoing any indemnification rights of PG&E in this DPA are additive to any rights at law or in equity that PG&E has under the Agreement.

23. **CONFLICTS.** In the event any term in this DPA is inconsistent or contradicts the terms in any other agreement between the Parties, the terms in this DPA shall apply.

24. **MISCELLANEOUS**. This DPA constitutes the entire agreement and understanding of the Parties with respect to the subject matter hereof, and its terms shall govern the event of any inconsistency between this DPA and any other agreement between the Parties. This DPA shall be amended only by a written agreement between the Parties that specifically references this DPA by name. Company's obligations hereunder shall survive the termination of the service agreements between the parties and the completion of any and all services performed thereunder.