DATA SECURITY AGREEMENT

THIS DATA SECURITY AGREEMENT, including Exhibits attached hereto and made a part hereof ("Agreement") which are incorporated by reference herein, is made as of this _____ day of _____ , 20___ by and between Central Hudson Gas & Electric Corporation, a New York corporation with offices at 284 South Avenue, Poughkeepsie, New York 12601 ("Utility") and _____, a Community Choice Aggregator ("CCA") with offices at _____; and together with Utility the ("Parties" and each, individually, a "Party").

RECITALS

WHEREAS, CCA desires to have access to certain utility customer information, either customer-specific or aggregated customer information in order to administer a community choice aggregation program ("CCA Program") for the benefit of its members in accordance with the New York State Public Service Commission's ("Commission") Order Authorizing Framework for Community Choice Aggregation Opt-Out Program (the "Order") in Case 14- M-0224 (effective April 21, 2016);; and

WHEREAS, (i) the Order directs Utility to provide to CCA certain aggregated and anonymized information of Utility's residential and small commercial customers that do not currently take service from an energy services company ("ESCO") and are located within CCA's service area, including, without limitation, aggregated usage and capacity tag information as well as certain Customer-Specific Information applicable to such customers, including, without limitation, all customer specific information such as, but not limited to, name, address and utility account number (or Point of Delivery Identifier) for the sole and limited purpose of facilitating the CCA Program and (ii) Utility may assess a reasonable fee in connection with its provision of such information as set forth in the Utility's tariff or as otherwise approved by the Commission; and

WHERAS, Utility and CCA also desire to enter into this Agreement to establish, among other things, the obligations of the CCA with respect to such Confidential Utility Information and the price at which the CCA may acquire access to the Confidential Utility Information; and

NOW, THEREFORE, in consideration of the premises and of the covenants herein contained, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties, intending to be legally bound, hereby agree as follows:

1. Definitions.

a. Customer-Specific Information" shall have the meaning attributed to it in the Recitals.

b. "CCA" shall have the meaning attributed to it in the Recitals.

c. "Confidential Utility Information" means, collectively, aggregated and customer-specific information that Utility is: (A) required by the Commission to provide to CCA and (B) any other Utility-specific, aggregated, Personal Data,

Sensitive Data, or Utility Data, or customer-specific data provided to CCA by Utility.

d. "Data Protection Requirements" means, collectively, (A) all national, state, and local laws, regulations, or other government standards relating to the protection of information that identifies or can be used to identify an individual that apply with respect to CCA or its Representative's Processing of Confidential Utility Information; (B) the Utility's internal requirements and procedures relating to the protection of information that identifies or can be used to identify an individual that apply with respect to CCA or its Representative's Processing of Confidential Utility Information; and (C) the Commission rules, regulations, and guidelines relating to confidential data, including the Commission-approved Uniform Business Practices ("UBPs").

e. "Data Security Incident" means a situation when CCA reasonably believes that there has been: (A) the loss or misuse (by any means) of Confidential Utility Information; (B) the inadvertent, unauthorized and/or unlawful Processing, corruption, modification, transfer, sale or rental of Confidential Utility Information; (C) any other act or omission that compromises the security, confidentiality, or integrity of Confidential Utility Information or (D) any breach of any Data Protection Requirements in relation to the Processing of Confidential Utility Information by CCA or any current or former Representatives.

f. "Destroy" means (A) shredding; (B) permanently erasing and deleting; (C) degaussing; or (D) otherwise modifying Confidential Utility Information in paper, electronic, or other means so as to make it unreadable, unreconstructible, and indecipherable. All Confidential Utility Information as may be specifically requested by Utility must be disposed of in a manner described in (A) through (D) herein.

g. "ESCO" shall have the meaning set forth in the Recitals.

h. "Personal Data" means any information that can be used to identify, locate, or contact an individual, including an employee, customer, or potential customer of Utility, including, without limitation: (A) first and last name; (B) home or other physical address; (C) telephone number; (D) email address or online identifier associated with an individual; (E) "Sensitive Data" as defined below; (F) ZIP codes; (G) employment, financial, or health information; or (H) any other information relating to an individual, including cookie information and usage and traffic data or profiles, that is combined with any of the foregoing.

i. "Commission" shall have the meaning attributed to it in the Recitals.

j. "Processing" (including its cognate, "process") means any operation, action, error, omission, negligent act, or set of operations, actions, errors, omissions, or negligent acts that is performed using or upon Personal Data or Utility Data, whether it be by physical, automatic or electronic means, including, without

limitation, collection, recording, organization, storage, access, adaptation, alteration, retrieval, use, transfer, hosting, maintenance, handling, retrieval, consultation, use, disclosure, dissemination, exfiltration, taking, removing, copying, processing, making available, alignment, combination, blocking, deletion, erasure, or destruction.

k. "Sensitive Data" is that subset of Personal Data, including Social Security number, passport number, driver's license number, Utility customer account number, Municipal Identification (NYCID), or similar identifier.

l. "Third-Party Representatives" or "Representatives" means those agents of CCA that are contractors or subcontractors.

m. "Utility Data" means data held by Utility, whether produced in the normal course of business or at the request of CCA or a CCA and whether or not it is provided to CCA.

2. Scope of the Agreement. This Agreement shall govern and apply to all Confidential Utility Information disclosed to CCA or to which CCA is given access by Utility, including all archival or back-up copies of the Confidential Utility Information held or maintained by CCA (or it its Representatives). All Confidential Utility Information, in whatever form, media, or medium provided or held, and all extracts, compilations, studies, or other documents based on, derived from, or containing Confidential Utility Information, all data electronically exchanged between the Parties, and all correspondence between or among the Parties or their respective Representatives pertaining to the same shall constitute Confidential Utility Information hereunder. No financial information will be provided pursuant to this Agreement. If any information is inadvertently sent to CCA, CCA will immediately notify the Utility and Destroy any such information in the appropriate manner.

3. Provision of Information. Utility agrees to provide to CCA or its Representatives, certain Confidential Utility Information, as requested, provided that (i) CCA and its Representatives are in compliance with the term of this Agreement; (ii) CCA has provided and has caused its Representatives to provide, to the satisfaction of Utility any Vendor Product/Service Security Assessments, attached hereto as Exhibit A or such other risk assessment forms as Utility may require from time to time ("The Assessment") and CCA will comply with the utility data protection program; (iii) CCA (and its Representatives, as applicable) shall have and maintain throughout the term systems and processes in place and as detailed in the assessment acceptable to Utility to protect Confidential Utility Information; (iv) CCA complies and shall cause its Third Party Representatives to comply with Utility's data protection programs; and (v) Utility receives written confirmation from New York State Department of Public Service Staff that certain prerequisites identified in the Order have been satisfied. Provided the foregoing prerequisites have been satisfied, Utility shall within twenty (20) days of receipt of CCA's written request for such Confidential Utility Information, provide such Confidential Utility Information as required by the Order. Specifically, Utility shall provide, as requested by the

CCA, aggregated data, including the number of customers by service class, the aggregated peak demand (kW) (for electricity) by month for the past 12 months, by service class to the extent possible, and the aggregated energy (kWh) for electricity or volumetric consumption for gas by month for the past 12 months by service class and customer-specific data, including the customer of record's name, mailing address, account number, and primary language and any customer-specific alternate billing name and address, to the extent available. Unless the Parties otherwise agree, the provision of Confidential Utility Information by Utility shall be effectuated electronically, as a file transfer made via encrypted FTP or other secure process acceptable to Utility.

4. **Confidentiality.** CCA shall: (A) hold all Confidential Utility Information in strict confidence; except as otherwise expressly permitted by Section 7 herein; (B) not disclose Confidential Utility Information to any other person or entity (including but not limited to subcontractors, affiliates, or members of CCA); (C) not Process Confidential Utility Information outside of the United States; (D) not Process Confidential Utility Information other than for the Services defined in the Recitals as authorized by this Agreement; (E) limit reproduction of Confidential Utility Information; (F) store Confidential Utility Information in a secure fashion at a secure location in the United States that is not accessible to any person or entity not authorized to receive the Confidential Utility Information under the provisions hereof; (G) otherwise use at least the same degree of care to avoid publication or dissemination of the Confidential Utility Information as CCA employs (or would employ) with respect to its own confidential information that it does not (or would not) desire to have published or disseminated, but in no event less than reasonable care; and (H) to the extent required by the Utility, each person with a need to know the Confidential Information shall sign the Third-Party Representative Agreement set forth as Exhibit B to this Agreement. At all times, Utility shall have the right to request further assurances that the foregoing restrictions and protections concerning Confidential Utility Information are being observed and CCA shall be obligated to promptly provide Utility with the requested assurances.

5. **Exceptions Allowing CCA to Disclose Confidential Utility Information.**

   a. **Disclosure to Representatives**. Notwithstanding the provisions of Section 6 herein, CCA may disclose Confidential Utility Information to its contractors or subcontractors who have a legitimate need to know or use such Confidential Utility Information for the sole and limited purposes of providing Services, provided that each such Representative first (A) is advised by CCA of the sensitive and confidential nature of such Confidential Utility Information; (B) agrees to comply with the provisions of this Agreement, provided that with respect to Representatives and this subsection (B), such Representatives must agree in writing to be bound by and observe the provisions of this Agreement as though such Representatives were CCA; and (C) signs the Representative Agreement. All such written agreements with Representatives shall include direct liability for the Representatives towards Utility for breach thereof by the Representatives, and a copy of such agreement and each Representative

Agreement and CCA agreement shall be made available to Utility upon request. Notwithstanding the foregoing, CCA shall be liable to Utility for any act or omission of a Representative, including without limitation, Representatives that would constitute a breach of this Agreement if committed by CCA.

b. **Disclosure if Legally Compelled**. Notwithstanding anything herein, in the event that CCA or any of its Representatives receives notice that it has, will, or may become compelled, pursuant to applicable law or regulation or legal process to disclose any Confidential Utility Information (whether by receipt of oral questions, interrogatories, requests for information or documents in legal proceedings, subpoenas, civil investigative demands, other similar processes, or otherwise), CCA shall, except to the extent prohibited by law, within 24 hours notify Utility, orally and in writing, of the pending or threatened compulsion. To the extent lawfully allowable, Utility shall have the right to consult with CCA and the Parties will cooperate, in advance of any disclosure, to undertake any lawfully permissible steps to reduce and/or minimize the extent of Confidential Utility Information that must be disclosed. Utility shall also have the right to seek an appropriate protective order or other remedy reducing and/or minimizing the extent of Confidential Utility Information that must be disclosed. In any event, CCA and its Representatives shall disclose only such Confidential Utility Information which they are advised by legal counsel that they are legally required to disclose in order to comply with such applicable law or regulation or legal process (as such may be affected by any protective order or other remedy obtained by Utility) and CCA and its Representatives shall use all reasonable efforts to ensure that all Confidential Utility Information that is so disclosed will be accorded confidential treatment.

6. **Return/Destruction of Information**. Within ten (10) days after Utility's written demand, CCA shall (and shall cause its Representatives to) cease to access and Process Confidential Utility Information and shall at the Utility's option: (A) return such Confidential Utility Information to Utility in such manner, format, and timeframe as reasonably requested by Utility or, if not so directed by Utility, (B) Destroy all copies of all Confidential Utility Information (including any and all extracts, compilations, studies, or other documents based upon, derived from, or containing Confidential Utility Information) that has come into CCA's or its Representatives' possession, including destroying Confidential Utility Information from all systems, records, archives, and backups of CCA and its Representatives, and all subsequent access, use, and Processing of the Confidential Utility Information by CCA and its Representatives shall cease. Notwithstanding the foregoing, CCA and its Representatives shall not be obligated to erase Confidential Utility Information contained in an archived computer system backup maintained in accordance with their respective security or disaster recovery procedures, provided that CCA and its Representatives shall (1) not have experienced a Data Security Incident, (2) not permit access to or recovery of Confidential Utility Information from such computer backup system and (3) keep all such Confidential Utility Information confidential in accordance with this Agreement. CCA shall, upon request, certify to Utility that the destruction by CCA and its Representatives

required by this Section has occurred by (A) having a duly authorized officer of CCA complete, execute, and deliver to Utility a certification and (B) obtaining substantially similar certifications from its Representatives and maintaining them on file. Compliance with this Section 8 shall not relieve CCA from compliance with the other provisions of this Agreement. The obligations under this Section shall survive any expiration of termination of this Agreement.

7. **Audit.** Upon reasonable notice to CCA, CCA shall, and shall require its Representatives to permit Utility, its auditors, designated audit representatives, and regulators to audit and inspect, at Utility's sole expense (except as otherwise provided in this Agreement), and no more often than once per year (unless otherwise required by Utility's regulators): (A) the facilities of CCA and CCA's Representatives where Confidential Utility Information is Processed by or on behalf of CCA; (B) any computerized or paper systems used to Process Confidential Utility Information; and (C) CCA's security practices and procedures, facilities, resources, plans, procedures, and books and records relating to the privacy and security of Confidential Utility Information. Such audit and inspection rights shall be, at a minimum, for the purpose of verifying CCA's compliance with this Agreement, including all applicable Data Protection Requirements. Notwithstanding anything herein, in the event of a Data Security Incident, CCA shall and shall cause its Representatives to permit an audit hereunder more frequently than once per year, as may be requested by Utility. CCA shall immediately correct any deficiencies identified by Utility.

8. **Investigation.** Upon notice to CCA, CCA shall assist and support Utility in the event of an investigation by any regulator or similar authority, if and to the extent that such investigation relates to Confidential Utility Information Processed by CCA on behalf of Utility. Such assistance shall be at Utility's sole expense, except where such investigation was required due to the acts or omissions of CCA or its Representatives, in which case such assistance shall be at CCA's sole expense.

9. **Data Security Incidents.** CCA is responsible for any and all Data Security Incidents involving Confidential Utility Information that is Processed by, or on behalf of, CCA. CCA shall notify Utility in writing immediately (and in any event within twenty-four (24) hours) whenever CCA reasonably believes that there has been a Data Security Incident. After providing such notice, CCA will investigate the Data Security Incident, and immediately take all necessary steps to eliminate or contain any exposure of Confidential Utility Information and keep Utility advised of the status of such Data Security Incident and all matters related thereto. CCA further agrees to provide, at CCA's sole cost, reasonable assistance and cooperation requested by Utility and/or Utility's designated representatives, in the furtherance of any correction, remediation, or investigation of any such Data Security Incident and/or the mitigation of any damage, including any notification required by law or that Utility may determine appropriate to send to individuals impacted or potentially impacted by the Data Security Incident, and/or the provision of any credit reporting service required by law or that Utility deems appropriate to provide to such individuals. Unless required by law, CCA shall not notify any

individual or any CCA other than law enforcement of any potential Data Security Incident involving Confidential Utility Information without first consulting with, and obtaining the permission of, Utility. In addition, within 30 days of identifying or being informed of a Data Security Incident, CCA shall develop and execute a plan, subject to Utility's approval, that reduces the likelihood of a recurrence of such Data Security Incident. CCA agrees that Utility may at its discretion and without penalty immediately suspend performance hereunder and/or terminate the Agreement if a Data Security Incident occurs.

10. **No Intellectual Property Rights Granted.** Nothing in this Agreement shall be construed as granting or conferring any rights, by license, or otherwise, expressly, implicitly, or otherwise, under any patents, copyrights, trade secrets, or other intellectual property rights of Utility, and CCA shall acquire no ownership interest in the Confidential Utility Information (which, as between CCA and Utility, shall be and remain the proprietary and confidential information of Utility). No rights or obligations other than those expressly stated herein shall be implied from this Agreement.

11. **Additional Obligations.**

a. CCA shall not create or maintain data which are derivative of Confidential Utility Information except for the purpose of performing its obligations under this Agreement or as authorized by Utility. Data collected by CCA from customers through its website or other interactions based on those customers' interest in receiving information from or otherwise engaging with CCA or its partners shall not be considered Confidential Utility Information or a derivative of Confidential Utility Information for the purpose of this Agreement.

b. CCA shall comply with all applicable privacy and security laws to which it is subject, including without limitation all applicable Data Protection Requirements and not, by act or omission, place Utility in violation of any privacy or security law known by CCA to be applicable to Utility.

c. CCA shall have in place appropriate and reasonable processes and systems, including an Information Security Program to protect the security of Confidential Utility Information and prevent a Data Security Incident, including, without limitation, a breach resulting from or arising out of CCA's internal use, Processing, or other transmission of Confidential Utility Information, whether between or among CCA's Representatives, subsidiaries and affiliates or any other person or entity acting on behalf of CCA, including without limitation Representatives.

d. CCA shall safely secure or encrypt all Confidential Utility Information during storage or transmission.

e. CCA shall establish policies and procedures to provide reasonable and prompt assistance to Utility in responding to any and all requests, complaints, or other communications received from any individual who is or may be the subject of

a Data Security Incident involving Confidential Utility Information Processed by CCA to the extent such request, complaint or other communication relates to CCA's Processing of such individual's Confidential Utility Information.

f. CCA shall establish policies and procedures to provide all reasonable and prompt assistance to Utility in responding to any and all requests, complaints, or other communications received from any individual, government, government agency, regulatory authority, or other entity that is or may have an interest in the Confidential Utility Information, data theft, or other unauthorized release of Confidential Utility Information, disclosure of Confidential Utility Information, or misuse of Confidential Utility Information to the extent such request, complaint or other communication relates to CCA's accessing or Processing of such Confidential Utility Information.

12. **Payment.** In consideration of Utility's agreement to provide Confidential Utility Information in accordance with Section 2, CCA shall pay to Utility fees pursuant to its tariffs.

13. **Specific Performance.** The Parties acknowledge that disclosure or misuse of Confidential Utility Information in violation of this Agreement may result in irreparable harm to Utility, the amount of which may be difficult to ascertain and which may not be adequately compensated by monetary damages, and that therefore Utility shall be entitled to specific performance and/or injunctive relief to enforce compliance with the provisions of this Agreement. Utility's right to such relief shall be in addition to and not to the exclusion of any remedies otherwise available under this Agreement, at law or in equity, including monetary damages, the right to terminate this Agreement for breach and the right to suspend the provision or Processing of Confidential Utility Information hereunder. CCA agrees to waive any requirement for the securing or posting of any bond or other security in connection with Utility obtaining any such injunctive or other equitable relief and hereby authorizes, to the extent lawfully possible, any court of competent jurisdiction to dispense with any requirement for such bond or other security which might otherwise be judicially imposed.

14. **Indemnification.** To the fullest extent permitted by law, CCA shall indemnify and hold Utility, its affiliates, and their respective officers, directors, trustees, shareholders, employees, and agents, harmless from and against any and all loss, cost, damage, or expense of every kind and nature (including, without limitation, penalties imposed by the Commission or other regulatory authority or under any Data Protection Requirements, court costs, expenses, and reasonable attorneys' fees) arising out of, relating to, or resulting from, in whole or in part, the breach or non-compliance with this Agreement by CCA or any of its Representatives.

15. **Notices.** With the exception of notices or correspondence relating to potential or pending disclosure under legal compulsion, all notices and other correspondence hereunder shall be sent by first class mail, by personal delivery, or by a nationally recognized courier service. Notices or correspondences relating to potential or pending disclosure under legal compulsion shall be sent by means of Express Mail

through the U.S. Postal Service or other nationally recognized courier service which provides for scheduled delivery no later than the business day following the transmittal of the notice or correspondence and which provides for confirmation of delivery. All notices and correspondence shall be in writing and addressed as follows:

If to CCA, to:

CCA Name:
Name of Contact:
Address:
Phone:
Email:

If to Utility, to:

Central Hudson Gas & Electric Corporation
Name of Contact: Katherine McIntosh
Address: 284 South Avenue
Poughkeepsie, New York 12601
Phone: (845) 486-5496
Email: kmcintosh@cenhud.com

A Party may change the address or addressee for notices and other correspondence to it hereunder by notifying the other Party by written notice given pursuant hereto.

16. **Term.** This Agreement shall be effective as of the date first set forth above and shall remain in effect until terminated by Utility upon not less than 10 days' prior written notice specifying the effective date of termination,; provided, however, that any expiration or termination shall not affect the respective obligations or rights of the Parties arising under this Agreement prior to the effective date of termination; and provided, further, that Utility may terminate this Agreement immediately upon notice to CCA in the event of a material breach hereof by CCA or its Representatives. For the purpose of clarity, a breach of Sections 4-10, 12-14, 17, and 25 shall be a material breach hereof. Upon the expiration or termination hereof, neither CCA nor its Representatives shall have any further right to Process Confidential Utility Information and shall immediately comply with its obligations under Section 8.

17. **Consent to Jurisdiction; Selection of Forum**. CCA irrevocably submits to the jurisdiction of the courts located within the State of New York with regard to any dispute or controversy arising out of or relating to this Agreement. CCA agrees that service of process on it in relation to such jurisdiction may be made by certified or registered mail addressed to CCA at the address for CCA pursuant to Section 11 hereof and that such service shall be deemed sufficient even under circumstances where, apart from this Section, there would be no jurisdictional basis for such service. CCA agrees that service of process on it may also be made

in any manner permitted by law. CCA consents to the selection of the New York State and United States courts within Dutchess County, New York as the exclusive forums for any legal or equitable action or proceeding arising out of or relating to this Agreement.

18. **Governing Law.** This Agreement shall be interpreted and the rights and obligations of the Parties determined in accordance with the laws of the State of New York, without recourse to such state's choice of law rules.

19. **Survival.** The obligations of CCA under this Agreement shall continue for so long as CCA and/or CCA's Representatives continue to have access to, are in possession of or acquire Confidential Utility Information even if all agreements between CCA and Utility have expired or been terminated.

20. **Counterparts.** This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which shall together constitute one and the same instrument. Copies of this Agreement and copies of signatures on this Agreement, including any such copies delivered electronically as a .pdf file, shall be treated for all purposes as originals.

21. **Amendments; Waivers.** This Agreement may not be amended or modified except if set forth in writing signed by the Party against whom enforcement is sought to be effective. No forbearance by any Party to require performance of any provisions of this Agreement shall constitute or be deemed a waiver of such provision or the right thereafter to enforce it. Any waiver shall be effective only if in writing and signed by an authorized representative of the Party making such waiver and only with respect to the particular event to which it specifically refers.

22. **Assignment.** This Agreement (and Aggregator's obligations hereunder) may not be assigned by CCA or Representatives without the prior written consent of Utility, and any purported assignment without such consent shall be void.

23. **Severability.** Any provision of this Agreement which is determined by any court or regulatory body having jurisdiction over this Agreement to be invalid or unenforceable will be ineffective to the extent of such determination without invalidating the remaining provisions of this Agreement or affecting the validity or enforceability of such remaining provisions.

24. **Entire Agreement.** This Agreement (including any Exhibits hereto) constitutes the entire agreement between the Parties with respect to the subject matter hereof and any prior or contemporaneous oral or written agreements or understandings with respect to such subject matter are merged herein. This Agreement may not be amended without the written agreement of the Parties.

25. **No Third-Party Beneficiaries.** This Agreement is solely for the benefit of, and shall be binding solely upon, the Parties and their respective agents, successors, and permitted assigns. This Agreement is not intended to benefit and shall not be for the benefit of any party other than the Parties and the indemnified parties

named herein, and no other party shall have any right, claim, or action as a result of this Agreement.

26. **Force Majeure.** No Party shall be liable for any failure to perform its obligations in connection with this Agreement, where such failure results from any act of God or other cause beyond such Party's reasonable control (including, without limitation, any mechanical, electronic, or communications failure) which prevents such Party from performing under this Agreement and which such Party is unable to prevent or overcome after the exercise of reasonable diligence.

27. **Relationship of the Parties.** Utility and CCA expressly agree they are acting as independent contractors and under no circumstances shall any of the employees of one Party be deemed the employees of the other for any purpose. Except as expressly authorized herein, this Agreement shall not be construed as authority for either Party to act for the other Party in any agency or other capacity, or to make commitments of any kind for the account of or on behalf of the other.

28. **Construction.** This Agreement shall be construed as to its fair meaning and not strictly for or against any party.

29. **Binding Effect.** No portion of this Agreement is binding upon a Party until it is executed on behalf of that Party in the space provided below and delivered to the other Party. Prior to such execution and delivery, neither the submission, exchange, return, discussion, nor the negotiation of this document, whether or not this document is then designated as a "draft" document, shall have any binding effect on a Party.

[signature page follows]

IN WITNESS WHEREOF, the Parties have executed and delivered this Agreement as of the date first above written.

CENTRAL HUDSON GAS & ELECTRIC CORPORATION	**___**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____

EXHIBIT A

Vendor Product/Service Security Assessments

Data Security Questionnaire

1. Is your computer network internal to your organization or do you have it hosted by a cloud / colocation vendor? If so, what vendor do you use?

2. What technical security measures has the vendor taken to protect its network? Please answer yes / no for each item.

    a. Firewall,
    b. Intrusion detection / prevention system,
    c. Anti-virus / anti-malware,
    d. Data loss prevention,
    e. Endpoint protection,
    f. etwork access control,
    g. Data encryption,
    h. Vulnerability scanning,
    i. Identity access management,
    j. Password management,
    k. Security alerting, audit logging, etc.,
    l. Remote access.

3. What procedural security measures has the vendor taken to protect its network? Please answer yes / no for each item. For each yes response, please provide a short description of your procedures. If no, please explain why you do not have this procedure / policy.

    a. Timely removal of terminated employees,
    b. Security awareness training including the use of phishing emails to test employees' application of training,
    c. Risk management program,
    d. Computer use policy,
    e. Incident response, disaster recovery, business continuity procedures and are these procedures tested annually,
    f. Defined process for implementing a system that includes proper security architecture / secure coding practices, pre-implementation testing, & vulnerability scanning.
    g. Change management controls,
    h. Patch management controls,
    i. Physical security controls over computer room,

j. Background and criminal checks on IT personnel,
k. Framework (CoBIT, ISO 27001, NIST),
l. Employee signed NDA,
m. Data privacy controls, etc.

4. How is the data transferred? Will it be encrypted in transit?

5. Where is the data physically located both production and backup data? (in the U.S. or foreign country)

6. How is the data stored and backed up? Will it be encrypted?

7. How do you ensure that unauthorized cyber and physical access is prevented?

8. Do you allow your employees to save Central Hudson data to a local or removable device or to print Central Hudson data?

9. Upon Central Hudson request, how would you either return or delete Central Hudson data (both electronic and hardcopy for production and backup systems)?

10. Are personnel able to access Central Hudson data from a mobile device? If so, what security measures have you taken to protect the device?

11. Do you have third party security assessments / audits performed on your network? (penetration test, vulnerability testing, SSAE 16 SOC 2 audit).

12. Do you have cyber insurance of $3 million?

13. Will the vendor use cloud computing software / hardware to provide the service? If yes, is the cloud service a: SaaS, PaaS, IaaS, private cloud, public cloud, community cloud, or hybrid cloud?

14. Has your company suffered from a security breach or data loss within the last 3 years. If yes, please describe the breach or data loss.

15. Does the vendor use outsourced third parties to assist in providing the service? If yes, did you perform a security review of that third party?

16. Has any of your third parties suffered from a security breach or data loss within the last 3 years. If yes, please describe the breach or data loss.

EXHIBIT A

Data Security Rider

I. General

(1) This Data Security Rider shall apply to Company in the event that Company is granted or has access, in any way, to Central Hudson's data and/or Confidential Information.

(2) Definitions:

i. "Cardholder Data" means a User's individual credit or debit card cardholder name, number, expiration date, the Card Security Code/Card Verification Value/Card Validation Code/Card Authentication Value, or Card Identification Number/Card Authentication Value 2/Card Validation Code 2/Card Verification Value 2.

ii. "Confidential Information" has the meaning set forth in this Agreement.

iii. "Customer Information" means a Central Hudson electric or gas delivery Central Hudson or Energy Service Company ("ESCO") customer's account number, name, address, zip code, phone number, email address, social security number, bank account number or routing number, credit card information, driver's license number, billing or usage data, enrollment in a low income or similar program, health status, including being on life support, meter Global Positioning System ("GPS") coordinates, or information regarding a customer's personal residence, such as square footage, smart appliances in residence, home network internet protocol address.

iv. "Cyber Event" means (a) any occurrence in an information system or network that has, or may potentially result in, unauthorized access, processing, corruption, modification, transfer or disclosure of data and/or Confidential Information or (b) a violation of an explicit or implemented Company security policy.

v. "Cyber Incident" means (a) the loss or misuse (by any means) of data and/or Confidential Information; (b) the inadvertent, unauthorized and/or unlawful access, processing, corruption, modification, transfer, disclosure, sale or rental of Confidential Information; or (c) any other act or omission that compromises the security, confidentiality, integrity, availability, or privacy of data and or Confidential Information protected by this Agreement.

vi. "Data" means all: (i) drawings, plans, maps, diagrams, charts, calculations, sketches, illustrations, designs and design layouts (collectively the "Drawings"), (ii) written technical specifications, design criteria, engineering data and all other information and data relating to the exchange of information between the Parties including Confidential Information, (iii) computer programs, software and source codes, (iv) operating and maintenance manuals with respect to the exchange of information, and (v) any other written or otherwise recorded

information relating to Agreement Exhibit 1; which are either annexed to or referred to in the Agreement or this Data Security Rider ("Rider") or required to be supplied by the Company pursuant to the terms of the Agreement Exhibit 1 and 2 or which Central Hudson may reasonably require in connection with this Agreement.

vii. "Personal Identifiable Information" ("PII") is defined as customer account number, name, address, phone number, electric or gas usage, billing amounts, social security numbers, driver's license number, credit card number, debit card number, or banking information.

viii. "Subcontractor" means any individual, firm or corporation engaged directly or indirectly by the Company in performance of any obligation pursuant to this Agreement, including any individual, firm or corporation that is an affiliate, agent, or assigned of Company.

ix. "Users" means a Central Hudson electric or gas delivery customer.

II. Privacy and Data Security

(1) Data and/or Confidential Information will at all times remain the sole property of the Party collecting the data and/or Confidential Information. Nothing in this Rider will be interpreted or construed as granting either Party any license or other right under any patent, copyright, trademark, trade secret, or other proprietary right or any right to assert any lien over or right to withhold from the other Party any Data and/or Confidential Information of the other Party.

(2) The Company shall provide annual security awareness training to any individual who has access to Central Hudson's data or who transmits data to Central Hudson ("Access Individuals"). Upon Central Hudson's request, the Company shall promptly provide to Central Hudson evidence that all Access Individuals have received such training.

(3) The Company must provide 20 business days prior written notice to Central Hudson if a new Subcontractor will be engaged by Company to support the data exchange with Central Hudson. The Company will assist Central Hudson in providing information, in form and substance sufficient to Central Hudson, regarding the state of the internal control environment of the Subcontractor to enable the Central Hudson to perform any security assessment that Central Hudson deems necessary. Central Hudson reserves the right to reject any proposed Subcontractor if the Subcontractor's internal control environment does not meet Central Hudson's requirements.

(4) The Company shall ensure that any Subcontractor is bound by terms and obligations at least as stringent as those set forth in this Agreement and Data Security Rider. Central Hudson reserves the right to audit such terms and obligations and to determine, in its sole discretion, whether or not the obligations and terms are sufficient.

(5) At any and all times during which Company or Subcontractor is engaged in data exchange with Central Hudson, Company and its Subcontractors will:

i. Have appropriate and reasonable security controls and/or measures in place to protect and safeguard the data exchange with Central Hudson from

disclosure or unauthorized access and/or use. The Company and its Subcontractors shall secure its computer systems, network, and devices using a defense-in-depth approach, compliant with industry recognized best practices or frameworks (e.g., NIST SP 800-53, ISO 27001 / 27002, COBIT, CIS Security Benchmarks, Top 20 Critical Controls, etc.).

ii. Have appropriate and reasonable privacy controls and/or measures to protect the data exchange with Central Hudson and Central Hudson's data according to industry recognized best practices or frameworks (e.g., DOE Data Guard Energy Data Privacy Program, AICPA Generally Accepted Privacy Principles, NISTIR 8062, ISO 29100, etc.).

iii. Comply with all applicable privacy and security laws, regulations, of New York State Public Service Commission Orders to which it or Central Hudson is subject and not, by act or omission, place Central Hudson in violation of any privacy or security law, regulation or order known by Company to be applicable to Central Hudson.

iv. Promptly notify Central Hudson of any material change(s) to the Company's security policies, procedures, controls or measures.

v. Safely secure or encrypt data during storage or transmission.

vi. Store data only within the boundaries of the United States.

vii. Except as may be necessary in connection with the data exchange, not store data on removable devices or media.

viii. Not back up data to the cloud without Central Hudson's prior written approval.

(6) If the Company uses a service provider or co-location data center, the Company will do so only if in compliance with the complementary user entity controls stated in the service provider's or co-location's SSAE 16 audit report.

(7) If the data exchange includes the use of the Company's hosted site(s), a privacy statement shall be present on the site that, at a minimum, includes the same language as in the Central Hudson's privacy statement located at: http://www.centralhudson.com/privacy/index.aspx.

(8) To the extent that the Company or Subcontractor processes credit card transactions as part of providing services and includes that data as part of the data exchange, the following requirements shall apply with respect to the Cardholder Data:

i. Company and its Subcontractor(s) represent that it is presently in compliance, and will remain in compliance with the Payment Card Industry Data Security Standard ("PCI DSS"), and all updates to PCS DSS, developed and published jointly by American Express, Discover, MasterCard and Visa ("Payment Card Brands") for protecting Cardholder Data.

ii. Company and its Subcontractor(s) acknowledges that Cardholder Data is owned exclusively by the data transmitter, credit card issuers, the relevant Payment Card Brand, and entities licensed to process credit and debit card transactions on behalf of Central Hudson, and further acknowledges that such Cardholder Data may be used solely to assist the foregoing parties in completing a transaction, supporting a loyalty program, providing fraud control services, or for other uses specifically required by law, the operating regulations

of the Payment Card Brands, or this Agreement, including this Data Security Rider.

iii. Company and its Subcontractor(s) agrees that, in the event of a Cyber Incident arising out of or relating to Company or Subcontractor's premises or equipment contained thereon, Company and Subcontractor shall provide full cooperation and access to its premises, books, logs and records by a designee of the Payment Card Brands to the extent necessary to perform a thorough security review and to validate Company's or Subcontractor's compliance with the PCI DSS.

(9) If Central Hudson wishes to discontinue the use of a hosted system and retrieve all Central Hudson Data, the Company and its Subcontractors shall ensure administrative interfaces and open APIs exist that provide access to all Central Hudson Data. With sufficient additional technical services resources and sufficient available bandwidth, all Central Hudson Data will be retrieved within 15 business days by Central Hudson and Central Hudson will authorize the Company and Subcontractor to delete the Data from within the hosted system in a manner consistent with the Agreement.

III. System Development

(1) To the extent that Company exchanges data with Central Hudson, the Company and its Subcontractors shall agree to apply the following requirements:

i. Establish policies and procedures that ensure the application system has been designed, built and implemented in a secure manner according to industry recognized best practices or frameworks (e.g., Build Security in Maturity Model (BSIMM) benchmarks, Open Group ACS Trusted Technology Provider framework, NIST, OWASP, etc.).

ii. Establish policies and procedures that ensure data security has been designed, built, and implemented into the application system according to industry recognized best practices or frameworks (e.g.,CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS, etc.).

iii. Establish policies and procedures that ensure the application system has been properly tested, including the development of a security test plan that defines an approach for testing or otherwise establishing that each of the security requirements has been met.

iv. Perform vulnerability assessment and penetration test on the application system to identify any security issues prior to the application system being placed into production. The Company or its Subcontractors verify that appropriate and reasonable action will be taken to mitigate any security issues identified prior to the system being placed into production.

v. Upon Central Hudson's request, the Company and each Subcontractor shall promptly provide the results of any vulnerability assessment and penetration test.

vi. Establish policies and procedures that ensure the application system has a proper change management and patch management process that includes

applying, testing, and validating the appropriate changes / patches before being placed in the production system.

vii. Upon Central Hudson's request, the Company and each Subcontractor shall promptly provide a self-certification letter to Central Hudson verifying that the application system meets the security requirements stated in the Data Security Rider, that all security activities have been performed, and all identified security issues have been documented and resolved.

(2) Company warrants that the application system contains no virus, Trojan, worm, undocumented shutdown mechanism or other code or feature which is intended, or is known by Company as likely, to disable, damage, destroy, deny access to or degrade the performance of the application system, or Confidential Information, Data or other information technology resource. Company warrants that the application system contains no backdoors or other feature that is intended to allow Company or someone else to gain unauthorized or surreptitious access to the application system or Data or other information technology resources. Company agrees to indemnify and hold Central Hudson harmless from any claims, damages, causes of action, costs and expenses arising out of or related to any breach of the warranty set forth in this Section.

IV. Incident Reporting

(1) It shall be presumed that the consequences of a virus, worm, Trojan, hacker intrusion or similar network security breach is not beyond the control of the Company or its Subcontractors.

(2) The Company shall remain responsible for any Cyber Event or Cyber Incident in relation to its or its Subcontractor's obligation set forth in the Agreement and Data Security Rider.

(3) The Company and their Subcontractors shall notify Central Hudson of a cyber-incident based on the Notification Table. Upon Central Hudson's request, the Company shall utilize and pay the cost for a computer forensic expert to investigate the incident that is either provided by the Company or Central Hudson.

Classification	Description	Notification By
Low	• System unavailable affecting 5% of Users.	Within 24 hours upon identification
Medium	• System unavailable affecting 10% of Users. • Cyber Event as defined in the Data Security Rider.	Within 8 hours upon identification
High	• System unavailable affecting 15% of Users. • Cyber Incident as defined in the Data Security Rider. • User request, complaint or other communication regarding potential misuse or unauthorized access to User's customer information.	Immediately upon identification

(4) The Company and its Subcontractors shall establish policies and procedures to properly investigate a Cyber Event or Cyber Incident and be willing to work with Central Hudson's forensic examiner.
(5) Notification will be made to the main contact at Central Hudson and to cybersecurity@cenhud.com.

V. Right to Audit

(1) Upon Central Hudson's request, the Company shall provide reasonable evidence that the controls of the Company and its Subcontractors include the proper security controls in place to protect Central Hudson's data and to ensure that the Company's Subcontractor's information systems related to the data exchange are operating effectively to ensure availability. The evidence may include, as determined by Central Hudson, CCA audit reports, such as the AICPA's SSAE 16 SOC 1 and SOC 2 (all 5 of the trust principles) reports or a penetration test report, or a certification letter from a CCA verifying that that the Company and its Subcontractors are in compliance, such as an ISO 27001 or PCI DSS certification letter.

Central Hudson may also, at its discretion, perform a security controls audit or penetration testing of the Company upon notice to the Company of not less than 30 business days. The Company shall include in each of its Contracts with each of its Subcontractors a right for Central Hudson to audit their services. The Company is responsible for addressing any user entity control requirements and any control deficiencies or findings that are noted in these audit reports.

EXHIBIT B

THIRD-PARTY REPRESENTATIVE AGREEMENT

I, _____, have read the Agreement between _____, ("Company") and Central Hudson Gas & Electric Corporation., ("Central Hudson") dated _____ __, 20__ (the "Agreement") and agree to the terms and conditions contained therein. My duties and responsibilities on behalf of _____ require me to have access to the Confidential Information disclosed by Central Hudson to the Company pursuant to the Agreement.

_____ _____