CONFIDENTIALITY AND NONDISCLOSURE AGREEMENT

This Confidentiality and Non-disclosure Agreement (the "Agreement") is made and entered into this __ th day of _____, 20__, by and between _____, a _____ ("Company") and Central Hudson Gas & Electric Corporation, a New York corporation ("Central Hudson"). _____ and Central Hudson may be referred to herein individually as a "Party" and collectively as the "Parties".

WITNESSETH:

A. The Company and Central Hudson are entering into this Agreement to govern the exchange of certain information for the purpose of evaluating, negotiating and/or consummating a project relating to _____ (the "Project").

B. In connection with the Project, the Company and Central Hudson will be exchanging, reviewing, and analyzing certain information, some or all of which could be considered Confidential Information (as such term is defined in Section 4 of this Agreement). As used in this Agreement, "Disclosing Party" shall mean the party that discloses its Confidential Information to the other party and "Receiving Party" shall mean the party that receives Confidential Information.

NOW THEREFORE, for and in consideration of the mutual exchange of Confidential Information to each other and in further consideration of the promises and the agreements herein contained, the sufficiency of which is hereby acknowledged and confessed, the Parties do hereby agree as follows:

1.Nondisclosure and Use of Confidential Information. Without the Disclosing Party's prior written consent, the Receiving Party shall not: (a) disclose to any third party the fact that the Disclosing Party has provided any Confidential Information to the Receiving Party; (b) disclose to any third party the Confidential Information or any portion thereof; or (c) use any Confidential Information for any purpose other than for the purpose stated in paragraph "A" above. The Confidential Information may be disclosed to Receiving Party's affiliates, directors, officers, employees, consultants, subcontractors and agents and its affiliates' directors, officers, employees, consultants, subcontractors and agents (collectively, "Representatives"), but only if each such Representative needs to know the Confidential Information in connection with the Project described above and signs the Individual Non-Disclosure Agreement ("INA") set forth as Attachment 1 to this Agreement. The Receiving Party shall provide a copy of each INA to the Disclosing Party within ten (10) business days after the INA is signed. The Confidential Information shall not be used by the Receiving Party or its Representatives for any purpose other than in connection with the Project. It is understood that (i) such Representatives shall be informed by the Receiving Party of the confidential nature of the Confidential Information and shall be required to adhere to the terms of this Agreement by the Receiving Party, and (ii) in any event, Receiving Party shall be responsible for any

breach of this Agreement by any of its Representatives. Receiving Party shall not disclose the Confidential Information in any form whatsoever to any person other than as permitted hereby, and shall safeguard the Confidential Information from unauthorized disclosure. For purposes hereof, "person" will be interpreted broadly to include any corporation, company, partnership, individual or governmental authority.

2.Standard of Care. The Receiving Party agrees to use at least the same care and discretion to avoid disclosure of the Disclosing Party's Confidential Information as it uses with its own similar information it does not wish to disclose, but in no event less than a reasonable standard of care; provided, however, that if the Disclosing Party requests that the Receiving Party employ specific measures against disclosure (*e.g.*, restrictions on copying), the Receiving Party shall agree to be bound by such measures by accepting the Confidential Information, provided that the Disclosing Party delivering the Confidential Information makes such request in writing on or before the date the Confidential Information is provided and identifies with specificity the Confidential Information that is to be subject to such specific measures. The Receiving Party shall promptly provide the Disclosing Party with notice of any actual or threatened breach of the terms of this Agreement or unauthorized disclosure of the Disclosing Party's Confidential Information.

3.Notice Preceding Compelled Disclosure. If Receiving Party or its Representatives are requested or required (by oral question, interrogatories, requests for information or documents, subpoena, civil investigative demand, or similar process) to disclose any Confidential Information, Receiving Party shall promptly notify Disclosing Party of such request or requirement so that Disclosing Party may seek an appropriate protective order. To the fullest extent permitted by law, Receiving Party agrees to cooperate with Disclosing Party to obtain an appropriate protective order. If, in the absence of a protective order or the receipt of a written waiver by the Disclosing Party, Receiving Party or its Representatives are compelled by a subpoena or by an order of a court of competent jurisdiction to disclose any portion of the Confidential Information or else stand liable for contempt or suffer other censure or penalty, Receiving Party and its Representatives may disclose only such portion(s) of the Confidential Information to the party compelling disclosure as is required by such subpoena or order and, in connection with such compelled disclosure, Receiving Party and its Representatives shall use their reasonable efforts to obtain from the party to whom disclosure is made written assurance that confidential treatment will be accorded to such portion(s) of the Confidential Information as is disclosed.

4.Definition of "Confidential Information". As used in this Agreement, "Confidential Information" means all information that is furnished to Receiving Party or its Representatives by Disclosing Party in the course of discussions or evaluations of the Project which concerns the Confidential Information, Disclosing Party, its partners or co-venturers, affiliates, or subsidiaries, and which is either confidential, proprietary, or otherwise not generally available to the public. Any information furnished to Receiving Party or its Representatives by a director, officer, employee, stockholder, partner, co-venturer, consultant, agent, or representative of Disclosing Party will be deemed

furnished by Disclosing Party for the purpose of this Agreement. The term "Confidential Information" shall specifically include, but shall not be limited to, the Disclosing Party's following information: business plans, strategies, forecasts and analyses; financial information; employee and vendor information; software (including all documentation and code), hardware, system designs, and protocols; product and service specifications; purchasing, logistics, sales, marketing and other business processes and energy infrastructure, information, location, quantity, production, flow, load, usage, size, capacity and/or other data or information; customer list, accounts, billing information and personal data including but not limited to names, addresses, telephone numbers, account numbers, dates of birth, social security numbers, employment information, and demographic, financial and transaction information ("Customer Information"); and all reports, analyses, notes or other information that are based on, contain or reflect any such information. Confidential Information also includes all information that by its nature should reasonably be expected to be treated as confidential, whether or not such information is identified as confidential.

5.Information Excluded from "Confidential Information". Notwithstanding any provision in this Agreement to the contrary, the following will not constitute Confidential Information for purposes of this Agreement: (i) information which is or becomes generally available to the public other than as a result of a disclosure by Receiving Party or its Representatives; (ii) information which was already known to Receiving Party on a non-confidential basis prior to being furnished to Receiving Party by Disclosing Party; (iii) information which becomes available to Receiving Party on a non-confidential basis from a source other than Disclosing Party or a representative of Disclosing Party if such source was not subject to any prohibition against transmitting the information to Receiving Party and was not bound by a confidentiality agreement with Disclosing Party; or (iv) information which was independently developed by the Receiving Party or its Representatives without reference to, or consideration of, the Confidential Information; provided however, that any specific Confidential Information, or any combination of features comprising the same, will not be deemed to fall within sub-paragraphs (i) to (iv) of this paragraph 5 inclusive, merely because the same is embraced by more general information or individual features which do fall within such paragraphs.

6.Return of Information. The Confidential Information shall, at all times, remain the property of Disclosing Party. At the Disclosing Party's sole discretion and immediately upon its request, all Confidential Information and any copies thereof shall be immediately returned to Disclosing Party or destroyed by Receiving Party (in which case an authorized representative of Receiving Party shall certify to such destruction in writing to Disclosing Party), and no copies will be retained by Receiving Party or its Representative unless the Parties agree otherwise in writing or unless required by any applicable laws or regulations governing document retention (in which case Receiving Party shall continue to keep such information confidential in accordance with the terms set forth herein). Any Confidential Information that may be found in drafts, notes, compilations, studies, synopses, or summaries thereof, or other documents prepared by or for Receiving Party or its Representatives, and written Confidential Information not so requested to be returned, will be held by Receiving Party and kept subject to the terms of this Agreement,

or destroyed. Notwithstanding the return or destruction of material, information and documents containing Confidential Information, the Receiving Party shall continue to be bound by the Receiving Party's obligations of confidentiality and other obligations hereunder.

7.No Waiver. No failure or delay in exercising any right, power or privilege hereunder will operate as a waiver thereof, nor will any single or partial exercise thereof preclude any other or further exercise thereof or the exercise of any other right, power, or privilege hereunder.

8.Remedies. Receiving Party acknowledges and agrees that money damages would not be a sufficient remedy for any breach of this Agreement by Receiving Party or its Representatives and Disclosing Party will be entitled to specific performance and injunctive relief as remedies for any such breach. Such remedies will not be deemed to be the exclusive remedies for a breach of this Agreement by Receiving Party or any of its Representatives but will be in addition to all other remedies available at law or in equity to Disclosing Party.

9.Indemnification and Defense. To the fullest extent permitted by law, the Receiving Party agrees to indemnify, defend, and hold the Disclosing Party, its Officers, Directors and employees free and harmless from any liability, damages, claims, causes of action, and/or litigation (including reasonable attorneys' fees) related to and/or arising out of any breach or default by Receiving Party of the terms, conditions or provisions of this Agreement, including but not limited to any claims made by the Disclosing Party's customers or any other third-party person or entity.

10.Duration. This Agreement shall remain in force and effect for one (1) year from the date first above written unless earlier terminated by either Party giving thirty (30) days written notice to the other, provided, however, that the restrictions on disclosure shall survive termination of the Agreement for a period of two (2) years from the date of expiry or termination of this Agreement or such longer period during which any Confidential Information retains its status as a trade secret or otherwise qualifies as confidential under applicable law. Notwithstanding the foregoing, sections 9 and 16 and the restrictions on disclosure for Customer Information shall remain binding for the fullest term permitted by law.

11.No Obligation or Joint Venture. The Parties hereto understand and agree that unless and until a definitive agreement has been executed and delivered, no contract or agreement providing for a project between the Parties shall be deemed to exist between the Parties, and neither Party will be under any legal obligation of any kind whatsoever with respect to such transaction by virtue of this or any written or oral expression thereof, except, in the case of this Agreement, for the matters specifically agreed to herein. For purposes of this Agreement, the term "definitive agreement" does not include an executed letter of intent, memorandum of understanding or any other preliminary written agreement or offer, unless specifically so designated in writing and executed by both Parties. This Agreement neither obligates a Party to deal exclusively with the other Party

nor prevents a Party or any of its affiliates from competing with the other Party or any of its affiliates. Either Party may terminate consideration and discussion of the Project at any time for any reason whatsoever, and the terminating party shall have no liability to the other party by reason of the termination; provided, however, that notwithstanding any such termination the Parties shall continue to be bound by the restrictions on disclosure detailed in this Agreement.

12.Independent Review. Neither Party makes any representation or warranty (express or implied) as to the accuracy or completeness of any Confidential Information provided by it hereunder, although each Party represents that it shall endeavor in good faith to provide information which is reliable and accurate, and each party agrees to assume full responsibility for all conclusions that it derives from its review of the Confidential Information. Nothing contained in this Agreement nor the conveying of Confidential Information hereunder shall be construed as granting or conferring any rights by license or otherwise in any intellectual property.

13.Publicity. Neither Party will use any logo, trademark, design, mark or any distinguishing feature of the other Party in any manner (including without limitation, in any advertising or promotional material) without the express prior written authorization of such other Party, which may be arbitrarily withheld.

14.Nondisclosure of Existence of Negotiations. Without the prior written consent of the other Party, or except as may be required by applicable law or regulation, each Party shall be prohibited from disclosing to any person, other than its Representatives who have a need to know such information in connection with the Project that the Confidential Information has been disclosed to the Receiving Party. Notwithstanding the foregoing sentence, neither Party shall be prohibited from disclosing the fact that discussions or negotiations are taking place between the Parties regarding the Project, provided that, neither Party shall disclose the substance or status of such discussions or negotiations.

15.Notices. All notices to be given to a party hereunder shall be in writing and delivered personally, by overnight courier, by mail or by facsimile, addressed as follows:

If to Central Hudson:

Central Hudson Gas & Electric Corporation
284 South Avenue
Poughkeepsie, NY 12601

Attention: _____

Title_____

Tel: (845) 486-_____
Facsimile: (845) 486-_____
Email: _____

If to _____:

Name
Address
City, State, Zip

Attention: _____

Title_____

Tel: _____
Fax: _____
Email: _____

Notices shall be deemed effective upon receipt. A Party may change its contact information by providing such information to the other Party in accordance with this Section 15.

16.Jurisdiction. This Agreement shall be governed by and construed in accordance with the laws of the State of New York, without regard to the conflict of laws principles thereof. For the limited purposes of the interpretation and/or enforcement of this Agreement, the Parties (a) consent and agree to the exclusive personal and subject matter jurisdiction of the New York State Supreme Court, County of Dutchess, in connection with any action or proceeding that relates to or arises from this Agreement, (b) consent to, and waive any objection to, the personal and subject matter jurisdiction of that court over any legal matter that relates to this Agreement, and (c) agree to service of process of any action commenced under this paragraph by FedEx to the addresses set forth in Section 15.

17.Cyber Insurance – Each Party receiving Confidential Information shall secure, provide and maintain during the term of this Agreement, an insurance policy that provides coverage for any and all liabilities, damages, claims, losses, costs and expenses, of any kind, that may be incurred by or asserted against the Central Hudson resulting from or related to:

(1) any act, error, or omission or negligence related to Company's technology and/or professional services;
(2) intellectual property infringement arising out of software and/or content;
(3) breaches of security;
(4) violation or infringement of any right to privacy, or any breach of federal, state, local or foreign security and/or privacy laws or regulations;
(5) theft, damage, destruction, or corruption of any data of Central Hudson or any employee, or customer of Central Hudson, including without limitation, unauthorized access, unauthorized use, identity theft, theft of personally

identifiable information or confidential corporate information, transmission of a computer virus or other type of malicious code; and

(6) participation, including a denial of service attack on a third party.

Minimum limits of $3,000,000 per occurrence.

Such insurance must cover all of the foregoing without limitation if caused by an independent Company working on behalf of the Company, in performing Services under this Agreement. The policy must be kept in force by Company during the term of this Agreement and for six (6) years (either as a policy in force or extended reporting period) after this Agreement is terminated or after completion of the Project provided for herein, whichever is later.

18.Company shall comply with the requirements set forth in the Data Security Rider, Attachment 2 to this Agreement and shall answer the questions set forth in the Vendor Questionnaire, Attachment 3 to this Agreement.

19.Miscellaneous. The Agreement inures to the benefit of the Parties hereto and their successors and assigns and is binding on each other and each other's successors and assigns; provided, however, that neither Party will assign this Agreement without the written consent of the other Party. This Agreement constitutes the entire agreement between the Parties hereto with respect to the subject matter hereof and supersedes and replaces any and all prior agreements and understandings with regard to the subject matter hereof. If any provision of this Agreement is held by a court of competent jurisdiction in a final, non-appealable judgment to be invalid, illegal or unenforceable, the remainder of the provisions of this Agreement shall remain in full force and effect and any invalid, illegal or unenforceable provision shall be replaced with a valid, legal or enforceable provision, the effect of which comes as close as possible to that of the invalid, illegal or unenforceable provision. The headings of the Sections of this Agreement are inserted for convenience only and do not constitute a part hereof or affect in any way the meaning or interpretation of this Agreement. This Agreement may be executed in multiple counterparts, each of which shall be deemed to be an original for all purposes. This Agreement may be executed by facsimile or reproductive signature and the Parties shall recognize, and not challenge, such execution as the valid and binding execution hereof. This Agreement may be modified only in a writing signed by both Parties.

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

[Insert Counterparty's Name]

By:_____

Name: _____

Title: _____

Central Hudson Gas & Electric Corporation

By:_____

Name: _____

Title: _____

ATTACHMENT 1

INDIVIDUAL NON-DISCLOSURE 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.

_____ _____

ATTACHMENT 2

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 the Confidential Information of Central Hudson.

(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 the agreement with the vendor.

iii. "Customer Information" means a customer's Central Hudson 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 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 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 Central Hudson 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 Confidential Information.

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 Services and/or Inputs, (iii) computer programs, software and source codes, (iv) operating and maintenance manuals with respect to the Services and/or Inputs, and (v) any other written or otherwise recorded data and information relating to the Scope of Services described in Exhibit A of the Agreement; 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 or Rider or which Central Hudson may reasonably require in connection with the construction, installation, use, operation, maintenance, repair, replacement or upgrading of the Services and/or Inputs.

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. "Services" has the meaning set forth in the agreement or statement of work.

ix. "Subcontractor" means any individual, firm or corporation engaged directly or indirectly by the Company in performance of any part of the Services, including any individual, firm or corporation that is an affiliate, agent, or assigned of Company.

x. "Users" means a Central Hudson electric or natural gas customer.

II. Privacy and Data Security

(1) Confidential Information and Data shall at all times remain the sole property of Central Hudson. Nothing in this Rider will be interpreted or construed as granting Company 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 Central Hudson any Confidential Information or Data of Central Hudson.

(2) The Company shall provide annual security awareness training to any individual who has access to PII of Central Hudson's customers. Upon Central Hudson's request, the Company shall promptly provide to Central Hudson evidence that individuals with access to any PII of Central Hudson's customers 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 Services that the Company is providing to 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 the 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 in possession of or processing Confidential Information, Company and its Subcontractors shall:

i. Have appropriate and reasonable security controls and/or measures in place to protect and safeguard the Confidential Information of Central Hudson and its Users 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 Central Hudson's Customer Information 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 Confidential Information during storage or transmission.

vi. Store Confidential Information only within the boundaries of the United States.

vii. Except as may be necessary in connection with providing Services, not store

Confidential Information on removable devices or media.

viii. Not back up Confidential Information 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 shall 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 Services provided include 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 Users' credit card transactions as part of providing the agreed upon Services, 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 Central Hudson, 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 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 Confidential Information and Data. With sufficient additional technical services resources and sufficient available bandwidth, all Confidential Information and Data will be retrieved within 15 business days by Central Hudson and Central Hudson will authorize the Company and Subcontractor to delete the Confidential Information and Data from within the hosted system in a manner consistent with the Agreement.

III. **System Development**

(1) To the extent that Company provides the Services, 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 Confidential Information, 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 paragraph.

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.

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 have the proper security controls in place to protect Central Hudson's Confidential Information and to ensure that the Company's Subcontractor's information systems related to the Services are operating effectively to ensure availability. The evidence may include, as determined by the Central Hudson, third party 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 third party verifying that that the Company and its Subcontractors are in compliance, such as an ISO 27001 or PCI DSS certification letter.

(2) Central Hudson may also, at its discretion, perform a security controls audit or penetration testing of the Company upon notice to the Company not less than 30 business days. The Company shall include in each of its Contracts with each of its Subcontractors a right for the 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.

ATTACHMENT 3

Vendor 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?
    a. Firewall,
    b. Intrusion detection / prevention system,
    c. Anti-virus / anti-malware,
    d. Data loss prevention,
    e. Endpoint protection,
    f. Network 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?
    a. Timely removal of terminated employees,
    b. Security awareness training – focus on phishing emails (required by PSC),
    c. Computer use policy,
    d. Incident response procedures,
    e. System pre-implementation testing,
    f. Change management controls,
    g. Physical security controls over computer room,
    h. Background checks on IT personnel,
    i. Framework (CoBIT, ISO 27001),
    j. Employee signed NDA,
    k. Data privacy controls, etc.
4. How is the data transferred? Will it be encrypted in transit?
5. Where is the data physically located? (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 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 $1 million?

13. Does the vendor use outsourced third parties to assist in providing the service?

14. Will the vendor use cloud computing software / hardware to provide the service?