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

If to _____:

Name
Address
City, State, Zip
Attention: Mr. _____
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 $5,000,000 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

This Data Security Rider (the "Rider") forms part of the Central Hudson Master/Professional (pickone) Services Agreement ("xxxx") that was entered into between Central Hudson Gas & Electric, (hereinafter, "Central Hudson") a corporation located at 284 South Avenue, Poughkeepsie, New York 12601-4879 and [INSERT CONTRACTOR], a corporation located at [INSERT ADDRESS, CITY, STATE, ZIP CODE] (hereinafter, "Contractor") (collectively, "Parties," or individually, "Party").

1. SCOPE

1.1 To the extent that the Contractor is collecting, using, disseminating, or retaining Confidential Information Nonpublic Information or BES Cyber Security Information, in any format, or is using or operating any Central Hudson Information Technology System or Operational Technology System, including a BES Cyber System, in order to perform its responsibilities or obligations pursuant to the Master Agreement, then this Rider shall apply in full.

1.2 In the event of a conflict between the terms and conditions of the Master Agreement and this Rider, the terms and conditions of this Rider shall supersede and control.

1.3 For the avoidance of doubt, any and all conditions, responsibilities, rights, obligations, and provisions set forth in the Master Agreement that are neither addressed nor contradicted by this Rider shall continue to apply in full.

2. DEFINITIONS

2.1 "Anomaly-Based Detection" means the process of comparing definitions of what activity is considered normal against observed events to identify significant deviations.

2.2 "Antispyware Software" means a program that specializes in detecting both malware and nonmalware
forms of spyware.

2.3 "Antivirus Software" means a program that monitors a computer or network to identify all major
types of malware and prevent or contain malware incidents.

2.4 "Authentication" means a process to verify the identity of a user, process, or device, as a prerequisite to allowing access to Confidential Information in a network/system.

2.5 "Availability" means the ability to ensure timely and reliable access to and use of information.

2.6 "Baseline Configuration" means a set of specifications for a system, or configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.

2.7 "BES Cyber Asset" means a Cyber Asset that if rendered unavailable, degraded, or misused would, within fifteen (15) minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

2.8 "BES Cyber Security Information" means information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.

2.9 "BES Cyber System" means one or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

2.10 "Business Days" means Monday through Friday, except for Federal legal public holidays as defined by 5 U.S.C. § 1603(a).

2.11 "Bulk Electric System," or "BES," means all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy.

2.12 "Cardholder" means the definition set forth by the Payment Card Industry Data Security Standard concerning a non-consumer or consumer customer to whom a payment card is issued to or any individual authorized to use the payment card.

2.13 "Cardholder Data" means the definition set forth by the Payment Card Industry Data Security Standard concerning information about a cardholder's primary account number, name, expiration date and/or service code.

2.14 "Confidential Information" means all business or technical information issued or provided by Central Hudson, including, technical data, trade secrets, know-how, ideas, research, prototypes, samples, formulas, compounds, methods, plans, specifications, characteristics, raw material data, software, discoveries, processes, designs, drawings, schematics, whether or not patentable, and information concerning Central Hudson's financial condition, product plans, services, customers, potential customers, distribution systems, suppliers, markets, business, technology, marketing plans, sales, manufacturing, purchasing and accounting methods, strategy, budgets, contracts, grants, costs, profits, employees and consultants, plans for future development, and other information of a similar nature, whether oral or in written form, or other tangible medium, and whether or not marked confidential. Confidential Information includes any and all Personal Data or any operational data outside of the scope of North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) collected, used, or retained by Contractor in order to perform its responsibilities or obligations pursuant to the Master Agreement.

2.15 "Confidentiality" means the preservation of authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

2.16 "Cryptographic Algorithm" means a well-defined computational procedure that takes variable inputs,
including a cryptographic key, and produces an output.

2.17 "Cyber Asset" means programmable electronic devices, including the hardware, software, and data in those devices.

2.18 "Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Confidential Information transmitted, stored or otherwise Processed.

2.19 "Element" means any electrical device with terminals that may be connected to other electrical devices such as a generator, transformer, circuit breaker, bus section, or transmission line. An Element may be comprised of one or more components.

2.20 "Encryption" means the conversion of plaintext to ciphertext through the use of a cryptographic algorithm.

2.21 "Identifiable Natural Person" means an individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name or an identification number.

2.22 "Integrity" means the act of safeguarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

2.23 "Malicious Code" means software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system, and may include a virus, worm, Trojan horse, or other code-based entity that infects a host.

2.24 "Malware" means a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system.

2.25 "Non-Public Information" means information that Contractor obtains from Central Hudson pursuant to the Master Agreement and/or this Rider that Contractor knows or reasonably should know has not been made available to the general public. Non-Public Information only refers to information that is neither Confidential Information or Personal Data.

2.26 "Network" mean a system implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

2.27 "Personal Data" means any information provided to or accessed by Contractor that relates to an Identifiable Natural Person.

2.28 "Security Controls" means the management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

2.29 "Security Control Baseline" means the set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.

2.30 "Spyware" means software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.

2.31 "Transmission" means an interconnected group of lines and associated equipment for the movement or transfer of electric energy between points of supply and points at which it is transformed for delivery to customers or is delivered to other electric systems.

3. DATA SECURITY STANDARDS

3.1 At any and all times that Contractor is performing a function on the behalf of Central

Hudson that involves the use or operation of a BES Cyber System that is subject to the NERC CIP Reliability Standards, the Contractor shall implement and maintain administrative, technical, and physical security measures that satisfy or exceed the minimal level of acceptable security as set forth in the NERC CIP Reliability Standards.

3.2 Except as provided in Section 3.2.a. of this Rider, at any and all times that Contractor is performing a function on the behalf of Central Hudson that involves the collection, use, storage, dissemination, processing, and/or retention of Confidential Information, it shall implement and maintain administrative, technical, and physical security measures described in Section 4 of this Rider.

a. To the extent that Contractor is performing a function on the behalf of Central Hudson that involves the collection, use, storage, dissemination, processing, and/or retention of Confidential Information that is (i) maintained on a BES Cyber System and (ii) subject to the NERC CIP Reliability Standards, Contractor shall implement and maintain administrative, technical, and physical security measures satisfy or exceed the minimal level of acceptable security as set forth in the NERC CIP Reliability Standards.

3.3 To the extent that Contractor is performing a function on the behalf of Central Hudson that involves the collection, use, storage, dissemination, processing, and/or retention of Non-Public Information that is not subject to Section 3.1 or 3.2 of this Rider, it shall implement reasonable information security measures to implement a defense in depth security posture, consistent with any applicable industry standards.

4. DATA SECURITY PROGRAM

4.1 Contractor shall maintain a data security program consisting of administrative, technical, and physical security measures designed to protect the confidentiality, integrity, and availability of Confidential Information, Non-Public Information and BES Cyber Security Information. The data security program shall be approved by an Officer of the Contractor Company.

4.2 The Contractor's data security program shall be based upon a risk assessment, which shall occur at least annually, that is designed to understand the internal and external risks, including cyber-based risks, to the Contractor's ability to maintain the confidentiality, integrity, and availability of Confidential Information or BES Cyber Security Information. The risk assessment described herein may be undertaken by the Contractor or a third-party at the Contractor's expense.

4.3 The data security program set forth in Section 4.1 shall include, as appropriate and based upon the risk assessment undertaken pursuant to Section 4.2, the following elements, as appropriate:

a. Risk Assessment: A process to identify and mitigate risks to Contractor's networks /

systems, Confidential Information or BES Cyber Security Information.

b. Data Classification and Asset Management. A process to identify and classify the collection, use, and retention of Confidential Information or BES Cyber Security Information, including where and how Confidential Information or BES Cyber Security Information is stored or otherwise maintained within Contractor's organization or stored at a subcontractor's location. It is the responsibility of the Contractor to maintain an inventory listing of where Central Hudson's Information is located.

c. Access Controls and Identity. A policy prescribing which individuals, including third-party vendors, are permitted to have access to a system or resource that contains Confidential Information or BES Cyber Security Information, and the scope to which such access is permitted. The policy should also include timely removal of access when it is no longer required.

d. Identification and Authentication. A process to identify, verify, and/or authenticate users accessing Confidential Information or BES Cyber Security Information. For remote administrative access, multi-factor authentication is used to access production environments.

e. Password Configuration: A policy to ensure passwords are complex, changed on a frequent basis, maintain a password history to prevent reuse of a previously used passwords, and account lockout parameter.

f. Awareness and Training. A program that provides security awareness training, at least annually, to any individual who has access to Confidential Information. The program shall maintain training attendance records and any applicable testing/exam products and results. Contractors with approved access to BES Cyber Security Information will receive quarterly cyber security awareness newsletter and is subject to successful completion of Central Hudson's NERC CIP training modules or vendor's own NERC CIP cyber security training if approved by Central Hudson.

g. Auditing and Accountability. A process for creating and maintaining system audit records to enable the monitoring, analysis, investigation, and reporting of network/system activity. Furthermore, the Contractor must ensure that the actions of a network/system users can be uniquely traced to that individual and that the control is operating effectively.

h. Configuration Management. A program to establish and maintain Baseline Configurations of Contractor's systems, including hardware, software, firmware, and documentation and to enforce Security Control Baselines for information technology products employed in Contractor's systems.

i. Media Protection. A program to protect system media, both paper and digital, including through appropriate Antispyware, Antivirus Software, and Encryption, to limit access to information on system media to authorized users, and to sanitize or destroy system media before disposal or release for reuse.

j. Incident Response Plan. A data breach incident response plan as described in Section 5 of this Rider.

k. Business Continuity and Disaster Recovery Plan: A plan to recover systems in the event of a disaster or cyber incident that results in extended unplanned downtime of systems. Contractor shall test the plan on at least a bi-annual basis.

l. System Maintenance. A program to perform periodic and timely maintenance, including but not limited to security or critical patches, on Contractor's networks/systems maintaining Confidential Information and to provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

m. Personnel Security. A program to verify that individuals occupying positions of responsibility concerning the collection, use, and retention of Confidential Information or BES Cyber Security Information are trustworthy and satisfy established security criteria, to ensure that networks/systems maintaining Confidential Information or BES Cyber Security Information are protected during and after personnel actions (e.g., terminations and transfers), and to sanction personnel failing to comply with Contractor's security policies and procedures.

n. Physical Protection. A process to limit physical access to networks/systems maintaining Confidential Information or BES Cyber Security Information to authorized individuals, to protect the physical infrastructure for such networks/systems, including against environmental hazards, and to provide appropriate environmental controls in facilities containing such networks/systems.

o. Security Assessment. A program to periodically assess the security requirements in Contractor's networks/systems maintaining Confidential Information or BES Cyber Security Information to determine if the requirements are effective in their application, to develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in such networks/systems, and to monitor security requirements on an ongoing basis to ensure the continued effectiveness of the requirements.

p. Communications Protection. A program and process to monitor, control, and protect communications and information transmitted or received by Contractor's networks/systems maintaining Confidential Information or BES Cyber Security Information at external and internal boundaries, including through Encryption, and

employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within such networks/systems.

q. Data Storage. A policy to ensure, to the greatest extent possible, that Confidential Information or BES Cyber Security Information is stored only within the boundaries of the United States or Canada; is properly protected and secured according to industry best practices; is not stored or maintained, except as may be necessary, on removable devices or media; and is not stored pursuant to a cloud storage provider without Central Hudson's prior written approval. Disposal of Confidential Information or BES Cyber Security Information must be approved by Central Hudson prior to disposal and done in a manner where erasing electronic media so that it cannot be read or reconstructed.

4.4 Contractor shall, as soon as reasonably possible, but in no event later than forty-eight (48) hours, notify Central Hudson of any material change to its data security program.

5. DATA BREACH INCIDENT RESPONSE PLAN

5.1 Contractor shall develop and maintain a Data Breach Incident Response Plan, which shall include the following elements:

a. Accountability. A designation of an individual who shall be responsible for implementing, maintaining, testing, and updating the Incident Response Plan.

b. Incident Response Team. The establishment of, and procedures for activating, an Incident Response Team, that has the authority and direction to respond to, resolve, or otherwise address an actual or reasonably suspected Data Breach.

c. Internal and External Resources. The identification of key internal and external resources, including outside counsel, crisis communications specialists, cyber forensic investigators, to assemble in order to assist in addressing an actual or reasonably suspected Data Breach.

d. Incident Detection. A program, including (as appropriate) automated-technical means, to enable the identification and documentation of Anomaly-Based Detections indicative of an actual or reasonably suspected Data Breach.

e. Response Procedures: A process to investigate incidents that includes collection and analysis techniques and chain-of-custody management that comply with industry standards for legally admissible forensic data and support the ability for litigation holds.

f. Recovery Plan. A process and program to contain the effects of a Data Breach, remediate any identified gaps, and recover to a normal state of business operations.

g. Post-Incident Review. A process to convene a post-Data Breach review team to consider the effectiveness and efficiency in detecting and responding to a Data Breach and provide recommendations on how to prevent a Data Breach from occurring in the future or improve the Incident Response Plan.

5.2 Contractor shall periodically train employees and other persons with access to Confidential Information or BES Cyber Security Information on the Data Breach Incident Response Plan, and the training shall emphasize how to recognize an actual or potential Data Breach, and the channels and means to report such incidents.

5.3 Tabletop Exercise: Contractor shall test the Data Breach Incident Response Plan and the Recovery Plan on at least an annual basis and within 15 calendar months of the last performed exercise.

6. NOTIFICATION OF DATA BREACH

6.1 Contractors shall notify Central Hudson's Cybersecurity Group at cybersecurity@cenhud.com, as soon as reasonably possible, but in no event later than forty-eight (48) hours, of any actual or reasonably suspected Data Breach after Contractor becomes aware of the incident.

6.2 The notification described in Section 6.1 shall, to the greatest extent possible, include the following elements:

a. A description of the nature of the Data Breach, including, where possible, the categories and approximate number of individuals affected.

b. A description of the likely consequences caused by the Data Breach.

c. A description of the measures taken or proposed to be taken to address the Data Breach, including, where appropriate, measures to mitigate its possible adverse impact on the victims or Central Hudson.

d. The name and contact details of the Contractor employee or representative from whom more information can be obtained.

6.3 Contractor shall provide, to the greatest extent possible, assistance to Central Hudson to assist in investigating or otherwise responding to any Data Breach.

6.4 Contractor shall provide, to the greatest extent possible, assistance to Central Hudson to enable it to meet any legal obligation it may have to notify any affected party, regulatory or governmental authority, or any other individual of the Data Breach.

6.5 Contractor shall be and remain liable for any Data Breach occurring during its or its

Subcontractor's activities undertaken pursuant to the Master Agreement and/or this Rider. Contractor agrees to indemnify and hold Central Hudson harmless from any claims, damages, cause of action, costs and expenses arising out of or related to any incident described in this Section.

7. THIRD PARTY SUBCONTRACTING

7.1 Central Hudson acknowledges and agrees that in order to satisfy the terms and conditions of the Master Agreement and/or this Rider, Contractor may contract with a third-party, subject to the following condition:

a. Contractor shall ensure that all third-party subcontractors agree, in writing, to be subject to the same, or substantially similar, terms and conditions set forth in this Rider as is the Contractor. Central Hudson reserves the right to audit such third-party subcontracts, at any time, to determine in its sole discretion whether this clause has been satisfied.

b. Contractor shall provide at least twenty (20) Business Days prior written notice to Central Hudson if a new third-party subcontractor will be engaged by Contractor to satisfy the terms and conditions of the Master Agreement and/or this Rider. Upon request by Central Hudson, the Contractor will provide Central Hudson information demonstrating that any proposed, or actual, third-party subcontractor, is capable of or is complying with the data security standards set forth herein, and Central Hudson reserves the right to reject any proposed Subcontractor if it cannot demonstrate such compliance.

c. Contractor shall ensure that all third-party subcontractors agree, in writing, to comply with all applicable data privacy and information security laws, regulations, and industry standards, including New York State Public Service Commission Orders to which it or Central Hudson is subject.

7.2 Contractor shall be and remain liable for any activity concerning a third-party subcontractor that violates the terms and conditions of the Master Agreement, this Rider, or any applicable data privacy and information security law, regulation, and industry standards. Contractor agrees to indemnify and hold Central Hudson harmless from any claims, damages, cause of action, costs and expenses arising out of or related to any incident described in this Section.

8. FINANCIAL INFORMATION AND DATA SECURITY

8.1 To the extent that Contractor is collecting, storing, processing, communicating or otherwise using Cardholder Data (within the meaning of Payment Card Industry Data Security Standard (PCI-DSS)) in order to perform its responsibilities or obligations pursuant to the Master Agreement and/or this Rider, it shall be responsible, in addition to any other

responsibilities and obligations set forth in this Rider, for the following:

a. Contractor shall create and maintain detailed, complete and accurate documentation describing the systems, processes, network segments, security controls, and dataflow used to receive, transmit, store and secure Cardholder Data, and such documentation shall conform with the applicable portions of the PCI-DSS in all material respects, as it has been amended from time-to-time.

b. Contractor will implement and maintain reasonable security measures to prevent the unauthorized access to Cardholder Data. These reasonable security measures shall satisfy or exceed the PCI-DSS.

c. Contractor will, no less than annually, test and evaluate the effectiveness of its security measures described in section 8.1.b of this Rider.

d. Notwithstanding Section 6.1 of this Rider, Contractor will notify Central Hudson, as soon as reasonably possible, but in no event later than fourty-eight48) hours, of any actual or reasonably suspected incident involving the unauthorized access to Cardholder Data, after Contractor becomes aware of the incident. The notification described in this subsection shall contain the elements set forth in Section 6.2(a)-(d) of this Rider.

e. Contractor shall report in writing to Central Hudson, at least annually, proof of compliance with PCI-DSS. If Contractor becomes aware that it, or its service providers, are not, or will not likely be, in compliance with PCI-DSS for any reason, Contractor will promptly report in writing to Central Hudson the non-compliance or likely non-compliance.

f. Contractor shall be and remain liable for any activity involving the unauthorized access to Cardholder data occurring during its or its Subcontractor's activities undertaken pursuant to the Master Agreement and/or this Rider. Contractor agrees to indemnify and hold Central Hudson harmless from any claims, damages, cause of action, costs and expenses arising out of or related to any incident described in this Section.

9. PROPRIETARY INFORMATION AND CONFIDENTIALITY

9.1 All Confidential Information, Non-Public Information and BES Cyber Security Information shall remain the property of Central Hudson and Contractor will not acquire any property rights in any of the information contained therein by virtue of such information being furnished to Contractor pursuant to the Master Agreement and/or this Rider.

9.2 All Confidential Information, Non-Public Information and BES Cyber Security Information furnished to Contractor shall be kept confidential by Contractor and used by

Contractor solely for the intended purpose or purposes for which it was furnished, and Contractor shall not disclose the content of any such to any third party; provided, however, that Contractor shall not be liable for:

a. The disclosure of any such information to a third party to the extent authorized, in writing, by Central Hudson.

b. The disclosure of any such information pursuant to a lawful subpoena or court order.

c. The disclosure of any such information to any third party subcontractor pursuant to Section 7 of this Rider.

d. The disclosure in the ordinary course of Contractor's business of any identical information which is in the public domain or which has been lawfully obtained by Contractor from third parties, provided that Contractor does not disclose that such information is also included as part of the duties performed in the Master Agreement and/or this Rider.

9.3 If Contractor is served with a subpoena, court order or other legally compelling demand (collectively, a "Demand") to produce, copy, furnish or allow the inspection of Confidential Information, Non-Public Information and BES Cyber Security Information or any portion thereof, Contractor agrees to immediately notify Central Hudson of the Demand so as to allow Central Hudson to seek a protective order or to contest the Demand, unless such notification is expressly prohibited by law. Nothing in this Section shall be deemed to require Contractor to violate any court order.

9.4 After completion and/or termination of the Master Agreement, Contractor shall either return all Confidential Information and Non-Public Information, and the copies thereof to Central Hudson, or destroy and certify the destruction of, all Confidential Information and Non-Public Information, unless otherwise prohibited by law. For BES Cyber Security Information, Contractor must complete Central Hudson's Contractor Acknowledgement of Return/Attestation of BES Cyber Security Information.

10. DATA PRIVACY AND CYBERSECURITY INSURANCE

10.1 If Contractor is subject to Section 3.1 or 3.2 of this Rider, is involved in the supply of or provision of information technology services including cloud services or if Contractor has access to any Confidential Information, BES Cyber Security Information, Non Public Information or Personal Data, it shall secure, provide and maintain during the term of the Contract, an insurance policy, with a minimum policy limit of $5,000,000 per occurrence, that provides coverage for any and all liabilities, damages, claims, losses, costs and expenses, of any kind, that may be incurred by Contractor resulting from or related to any of the following:

a. Any act, error or omission or negligence related to Contractor's technology and/or professional services.

b. Intellectual property infringement arising out of software and/or content.

c. Any Data Breach described herein.

d. Violation or infringement of any right to privacy, or any breach of federal, state, local or foreign security and/or privacy laws or regulations.

e. Theft, damage, destruction, or corruption of any data of Contractor or any employee, or customer of Contractor, including without limitation, unauthorized access, unauthorized use, identity theft, theft of Personal Data, Confidential Information, Non Public Information or BES Cyber Security Information, transmission of a computer virus or other type of malicious code, including a denial of service attack on a third party.

f. Participation, including a denial of service attack on a third party.

10.2 The insurance coverage described in Section 10.1 shall cover all of the foregoing without limitation if caused by Contractor or its Subcontract agent, assign or affiliate, including an independent contractor working on behalf of the Contractor, in performing any of its responsibilities or obligations pursuant to the Master Agreement and/or this Rider for six (6) years (either as a policy in force or extended reporting period) after this Rider is terminated or after completion of the Master Agreement, whichever is later.

11. COMPLIANCE AND AUDITS

11.1 Contractor shall use, process, transfer, share, and/or store Confidential Information, Non-Public Information or BES Cyber Security Information only within the scope of the Master Agreement and/or this Rider. Contractor shall not use Confidential Information, Non-Public Information or BES Cyber Security Information for any other purpose, unless expressly approved, in writing, by Central Hudson.

11.2 In performing its responsibilities or obligations pursuant to the Master Agreement and/or this Rider, Contractor shall comply with all applicable data privacy and information security laws, regulations, and industry or reliability standards, including New York State Public Service Commission Orders, New York State Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) or NERC CIP Reliability Standards to which it or Central Hudson is subject.

11.3 In the event that Contractor cannot, for whatever reason, comply with any applicable data privacy and information security law, regulation, and industry standard, it shall promptly

and in no case later than three (3) Business Days, notify Central Hudson of this situation and provide reason(s) for noncompliance.

11.4 Upon request, make available to Central Hudson within fourteen (14) Business Days all information necessary to demonstrate compliance with the obligations set forth in the Master Agreement and/or this Rider. To assist in demonstrating compliance, Contractor may furnish third party audit reports, penetration test reports, or a certification letter from a third party verifying that that the Contractor and its Subcontractor are in compliance with industry data security or reliability standards.

11.5 Central Hudson may, at its discretion, perform a security controls audit or penetration testing of Contractor, or its Subcontractor, after providing at least thirty (30) Business Days' notice to the Contractor. The Contractor is responsible for addressing any user entity control requirements and any control deficiencies or findings that are noted in these audit and testing reports.

12. EXPENSES AND FEES

12.1 Unless otherwise provided for herein, Contractor shall perform all the functions and activities described in this Rider, including all functions and activities that support Central Hudson in adhering to its legal obligations, at no extra cost or charge to Central Hudson and in accordance with existing fee and payment arrangements.

ACCEPTED AND AGREED TO BY EACH PARTY'S AUTHORIZED SIGNATORY:

Central Hudson Gas & Electric	**Contractor**
Signed:_____.	Signed:_____.
Printed:_____.	Printed:_____.
Title:_____.	Title:_____.
Date:_____.	Date:_____.

ATTACHMENT 3

Vendor Questionnaire – See stand-alone document

https://www.cenhud.com/globalassets/pdf/about-us/projects/bulk-energy-storage-june-10-2024/chge-appendix-d2-confidentiality-and-non-disclosure-agreement-2024-attachment-3-vendor-questionnaire.xlsx