

# **DATA SECURITY AGREEMENT**

This Data Security Agreement (“Agreement”) effective \_\_\_\_\_, is made and entered into this \_\_\_\_ day of \_\_\_\_\_, 20\_\_ by and between (“Utility”) and \_\_\_\_\_, an Energy Service Entity (“ESE”) with offices at \_\_\_\_\_; and together with Utility the (“Parties” and each, individually, a “Party”).

## RECITALS

WHEREAS, ESE desires to have access to certain utility customer information, either customer-specific or aggregated customer information, or the New York State Public Commission (“Commission”) has ordered Utility to provide to ESE customer information; and

WHEREAS, ESE has obtained consent from all customers from whom the ESE intends to obtain information from Utility; and

WHEREAS, Energy Services Company (“ESCO”), Direct Customer or Distributed Energy Resource (“DER”) Supplier may utilize a third party to fulfill its Service obligations, including but not limited to, Electronic Data Interchange (“EDI”) communications with Utility; and

WHEREAS, ESCO, Direct Customer or DER Supplier (“DERS”) utilization of a third party provider does not relieve ESCO, Direct Customer or DERS of their transactional obligation such that they must ensure that the third party provider must comply with all ESCO, Direct Customer or DERS obligations; and

WHEREAS, Utility and ESE also desire to enter into this Agreement to establish, among other things, the full scope of ESE’s obligations of security and confidentiality with respect to the Confidential Information in a manner consistent with the rules and regulations of the Commission and requirements of Utility; and

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

### 1. Definitions.

- a. “Confidential ESE Information” means information that ESE is: (A) required by the Uniform Business Practices (“UBP”) or DERS UBP (“UBP DERS”) to receive from the end use customer and provide to Utility to enroll the customer or (B) any other information provided by ESE to Utility and marked confidential by the ESE, but excludes (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; (iv) information which was independently developed by the Receiving Party or its Representatives without reference to, or consideration of, the Confidential Information; or (v) information provided by the customer with customer consent where the customer expressly agrees that the information is public.
- b. “Confidential Utility Information” means information that Utility is: (A) required by the UBP at Section 4: Customer information(C)(2), (3) or UBP DERS at Section 2C: Customer Data, to provide to ESCO, Direct Customer or DERS or (B) any other information provided to ESE by Utility and marked confidential by the Utility at the time of disclosure, but excludes (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; (iv) information which was independently developed by the Receiving Party or its Representatives without reference to, or consideration of, the Confidential Information; or (v) information provided by the customer with customer consent where the customer expressly agrees that the information is public.
- c. “Confidential Information” means, collectively, Confidential Utility Information or Confidential ESE Information.
- d. “Data Protection Requirements” means, collectively, (A) all national, state, and local laws, regulations, or other government standards relating to the protection of information that identifies or can be used to identify an individual that apply with respect to ESE or its Representative’s Processing of Confidential Utility Information; (B) industry best practices or frameworks to secure information, computer systems, network, and devices using a defense-in-depth approach, such as and including, but not limited to, NIST SP 800-53, ISO 27001 / 27002, COBIT, CIS Security Benchmarks, Top 20 Critical Controls as best industry practices and frameworks may evolve over time; and (C) the Commission rules, regulations, and guidelines relating to confidential data, including the Commission-approved UBP and UBP DERS.
- e. “Data Security Incident” means a situation when Utility or ESE reasonably believes that there has been: (A) the loss or misuse (by any means) of Confidential Information; (B) the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of Confidential Information, or Private Information as defined by GBL § 899-aa, computer systems, network and devices used by a business; (C) any other act or omission that compromises the security, confidentiality, or integrity of Confidential Information, or (D) any material breach of any Data Protection

Requirements in relation to the Processing of Confidential Information, including by any current or former Representatives.

- f. “DER Supplier” or “DERS” has the meaning set forth in the UBP DERS approved by the Commission and as it may be amended from time to time, which is “[a] supplier of one or more DERs that participates in a Commission authorized and/or utility or DSP-operated program or market. DERS may choose to provide DERs as standalone products or services, or may choose to bundle them with energy commodity. CDG Providers and On-Site Mass Market DG Providers are included within the definition of DERS. Entities which sell both DERs and energy commodity are both DERS and ESCOs.”
- g. “Direct Customer” has the meaning set forth in the UBP approved by the Commission and as it may be amended from time to time, which is “An entity that purchases and schedules delivery of electricity or natural gas for its own consumption and not for resale. A customer with an aggregated minimum peak connected load of 1 MW to a designated zonal service point qualifies for direct purchase and scheduling of electricity provided the customer complies with NYISO requirements. A customer with annual usage of a minimum of 3,500 dekatherms of natural gas at a single service point qualifies for direct purchase and scheduling of natural gas.”
- h. “ESCO” has the meaning set forth in the UBP approved by the Commission and as it may be amended from time to time, which is “an entity eligible to sell electricity and/or natural gas to end-use customers using the transmission or distribution system of a utility.”
- i. “ESE” shall have the meaning set forth in the Recitals and for the avoidance of doubt, includes but is not limited to ESCOs, Direct Customers, DERS and contractors of such entities with which Utility electronically exchanges data other than by email and any other entities with which Utility electronically exchanges data other than by email or by a publicly available portal.
- j. “PSC” or “Commission” shall have the meaning attributed to it in the Recitals.
- k. “Processing” (including its cognate, “process”) means any operation, action, error, omission, negligent act, or set of operations, actions, errors, omissions, or negligent acts that is performed using or upon Confidential Information or Utility Data, whether it be by physical, automatic or electronic means, including, without limitation, collection, recording, organization, storage, access, adaptation, alteration, retrieval, use, transfer, hosting, maintenance, handling, retrieval, consultation, use, disclosure, dissemination, exfiltration, taking, removing, copying, processing, making available, alignment, combination, blocking, deletion, erasure, or destruction.
- l. “Third-Party Representatives” or “Representatives” means those agents acting on behalf of ESCOs, Direct Customers, or DERS that are contractors or subcontractors and that store, transmit or process Confidential Utility

Information. For the avoidance of doubt, Third-Party Representatives do not include ESEs and their members, directors, officers or employees who need to know Confidential Utility Information for the purposes of providing Services.

- m. "Services" mean any assistance in the competitive markets provided by ESEs to end use customers or ESCOs, Direct Customers or DERS that also require interaction with a Utility, including but not limited to the electronic exchange of information with a Utility, and must be provided in accordance with the UBP or UBP DERS.
- n. "Utility Data" means data held by Utility, whether produced in the normal course of business or at the request of ESE.

- 2. **Scope of the Agreement.** This Agreement shall govern security practices of ESEs that have electronic communications, other than email, with the Utility and security practices that apply to all Confidential Utility Information disclosed to ESE or to which ESE is given access by Utility, including all archival or back-up copies of the Confidential Utility Information held or maintained by ESE (or its Representatives) and Confidential ESE Information. No financial information, other than billing information, will be provided pursuant to this Agreement. If any information is inadvertently sent to ESE or Utility, ESE or Utility will immediately notify the Utility/ESE and destroy any such information in the appropriate manner.
- 3. **ESE Compliance with all Applicable Commission Uniform Business Practices.** The Parties agree that the Commission's UBP and UBP DERS set forth rules governing the protection of Confidential Information and electronic exchange of information between the Parties, including but not limited to EDI.

\_\_\_\_\_ ESCO, Direct Customer or DERS utilizes a Third-Party Representative as a vendor, agent or other entity to provide electronic exchange of information, other than by email, with Utility ESE and will require Third-Party Representative to abide by the applicable UBP or UBP DERS.

- 4. **Customer Consent.** The Parties agree that the UBP and UBP DERS govern an ESE's obligation to obtain informed consent from all customers about whom ESE requests data from Utility. The ESE agrees to comply with the UBP and UBP DERS on customer consent and the Utility's tariffs regarding customer consent.
- 5. **Provision of Information.** Utility agrees to provide to ESE or its Representatives, certain Confidential Utility Information, as requested, provided that: (A) ESE and its Representatives are in compliance with the terms of this Agreement in all material respects; (B) if required by Utility, ESE has provided and has required its Representatives to provide, to the satisfaction of Utility any Vendor Product/Service Security Assessments or self-attestations (attached hereto as Exhibit A) or such other risk assessment forms as Utility may require from time to time ("Assessment") and ESE will comply with the Utility Assessment requirements as approved by the Utility; (C) ESE (and its Representatives, as applicable) shall have and maintain throughout the term, systems and processes in place and as

detailed in the Assessment acceptable to Utility to protect system security and Confidential Utility Information; and; (D) ESE complies and shall require its Third-Party Representatives who process Confidential Information to comply with Utility's Assessment requirements as approved by the Utility. Provided the foregoing prerequisites have been satisfied, ESE shall be permitted access to Confidential Utility Information and/or Utility shall provide such Confidential Utility Information to ESE. Nothing in this Agreement will be interpreted or construed as granting either Party any license or other right under any patent, copyright, trademark, trade secret, or other proprietary right or any right to assert any lien over or right to withhold from the other Party any Data and/or Confidential Information of the other Party. Utility will comply with the security requirements set forth in its Assessment.

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

Utility shall: (A) hold all Confidential ESE Information in strict confidence; except as otherwise expressly permitted by Section 7 herein; (B) not disclose Confidential ESE Information to any other person or entity except as set forth in Section 7(a) of this Agreement; (C) not Process Confidential ESE Information other than for the Services defined in the Recitals as authorized by this Agreement; (D) limit reproduction of Confidential ESE Information; (E) store Confidential ESE Information in a secure fashion at a secure location that is not accessible to any person or entity not authorized to receive the Confidential ESE Information under the provisions hereof; (F) otherwise use at least the same degree of care to avoid publication or dissemination of the Confidential ESE Information as Utility employs (or would employ) with respect to its own confidential information that it does not (or would not) desire to have published or disseminated, but in no event less than reasonable care; and (G) to the extent required by ESE, each Representative with

a need to know the Confidential ESE Information shall sign the Third-Party Representative Agreement set forth as Exhibit B to this Agreement. At all times, ESE shall have the right for cause to request reasonable further assurances that the foregoing restrictions and protections concerning Confidential ESE Information are being observed and Utility shall be obligated to promptly provide ESE with the requested assurances.

This Section 6 supersedes prior non-disclosure agreements between the Parties pertaining to Confidential Information.

## **7. Exceptions Allowing ESE to Disclose Confidential Utility Information.**

- a. **Disclosure to Representatives.** Notwithstanding the provisions of Section 6 herein, the Parties may disclose Confidential Information to their Third-Party Representatives who have a legitimate need to know or use such Confidential Information for the purposes of providing Services in accordance with the UBP and UBP DERS, provided that each such Third-Party Representative first: (A) is advised by the disclosing Party of the sensitive and confidential nature of such Confidential Information; (B) agrees to comply with the provisions of this Agreement, provided that with respect to Third-Party Representatives and this subsection (B), such Third-Party Representatives must agree in writing to be bound by and observe the provisions of this Agreement as though such Third-Party Representatives were a Party/ESE; and (C) signs the Third-Party Representative Agreement. All such written Agreements with Third-Party Representatives shall include direct liability for the Third-Party Representatives towards Utility/ESE for breach thereof by the Third-Party Representatives, and a copy of such Agreement and each Third-Party Representative Agreement shall be made available to Utility/ESE upon request. Notwithstanding the foregoing, the Parties shall be liable for any act or omission of a Third-Party Representative, including without limitation, those acts or omissions that would constitute a breach of this Agreement.
- b. **Disclosure if Legally Compelled.** Notwithstanding anything herein, in the event that a Party or any of its Third-Party Representatives receives notice that it has, will, or may become compelled, pursuant to applicable law or regulation or legal process to disclose any Confidential Information (whether by receipt of oral questions, interrogatories, requests for information or documents in legal proceedings, subpoenas, civil investigative demands, other similar processes, or otherwise), that Party shall, except to the extent prohibited by law, within one (1) business day, notify the other Party, orally and in writing, of the pending or threatened compulsion. To the extent lawfully allowable, the Parties shall have the right to consult and the Parties will cooperate, in advance of any disclosure, to undertake any lawfully permissible steps to reduce and/or minimize the extent of Confidential Information that must be disclosed. The Parties shall also have the right to seek an appropriate protective order or other remedy reducing and/or minimizing the extent of Confidential Information that must be disclosed. In any event, the Party and its Third-Party Representatives shall disclose only such Confidential Information which they are advised by legal

counsel that they are legally required to disclose in order to comply with such applicable law or regulation or legal process (as such may be affected by any protective order or other remedy obtained by the Party) and the Party and its Third-Party Representatives shall use all reasonable efforts to ensure that all Confidential Information that is so disclosed will be accorded confidential treatment.

- 8. Return/Destruction of Information.** Within thirty (30) days after Utility's written demand, ESE shall (and shall cause its Third-Party Representatives to) cease to access and Process Confidential Utility Information and shall at the Utility's option: (A) return such Confidential Utility Information to Utility in such manner, format, and timeframe as reasonably requested by Utility or, if not so directed by Utility, (B) shred, permanently erase and delete, degauss or otherwise modify so as to make unreadable, unreconstructible and indecipherable ("Destroy") all copies of all Confidential Utility Information (including any and all extracts, compilations, studies, or other documents based upon, derived from, or containing Confidential Utility Information) that has come into ESE's or its Third-Party Representatives' possession, including Destroying Confidential Utility Information from all systems, records, archives, and backups of ESE and its Third-Party Representatives, and all subsequent access, use, and Processing of the Confidential Utility Information by ESE and its Third-Party Representatives shall cease provided any items required to be maintained by governmental administrative rule or law or necessary for legitimate business or legal needs will not be destroyed until permitted and will remain subject to confidentiality during the retention period. ESE agrees that upon a customer revocation of consent, ESE warrants that it will no longer access through Utility Confidential Utility Information and that it will Destroy any Confidential Utility Information in its or its Third-Party Representative's possession. Notwithstanding the foregoing, ESE and its Third-Party Representatives shall not be obligated to erase Confidential Utility Information contained in an archived computer system backup maintained in accordance with their respective security or disaster recovery procedures, provided that ESE and its Third-Party Representatives shall: (1) not have experienced an actual Data Security Incident; (2) maintain Data Security Protections to limit access to or recovery of Confidential Utility Information from such computer backup system and; (3) keep all such Confidential Utility Information confidential in accordance with this Agreement. ESE shall, upon request, certify to Utility that the destruction by ESE and its Third-Party Representatives required by this Section has occurred by (A) having a duly authorized officer of ESE complete, execute, and deliver to Utility a certification and (B) obtaining substantially similar certifications from its Third-Party Representatives and maintaining them on file. Compliance with this Section 8 shall not relieve ESE from compliance with the other provisions of this Agreement. The written demand to Destroy or return Confidential Utility Information pursuant to this Section may occur if the ESE has been decertified pursuant to the UBP or UBP DERS, the Utility has been notified of a potential or actual Data Security Incident and Utility has a reasonable belief of potential ongoing harm or the Confidential Utility Information has been held for a period in excess of its retention period. The obligations under this Section shall survive any expiration of termination of this



Agreement. Subject to applicable federal, state and local laws, rules, regulations and orders, at ESE's written demand and termination of electronic exchange of data with Utility, Utility will Destroy or return, at ESE's option, Confidential ESE Information.

- 9. Audit.** Upon thirty (30) days notice to ESE, ESE shall, and shall require its Third-Party Representatives to permit Utility, its auditors, designated representatives, to audit and inspect, at Utility's sole expense (except as otherwise provided in this Agreement), and provided that the audit may occur no more often than once per twelve (12) month period (unless otherwise required by Utility's regulators). The audit may include (A) the facilities of ESE and ESE's Third-Party Representatives where Confidential Utility Information is Processed by or on behalf of ESE; (B) any computerized or paper systems used to Process Confidential Utility Information; and (C) ESE's security practices and procedures, facilities, resources, plans, procedures, and books and records relating to the privacy and security of Confidential Utility Information. Such audit rights shall be limited to verifying ESE's compliance with this Agreement, including all applicable Data Protection Requirements. If the ESE provides a SOC II report or its equivalent to the Utility, or commits to complete an independent third-party audit of ESE's compliance with this Agreement acceptable to the Utility at ESE's sole expense, within one hundred eighty (180) days, no Utility audit is necessary absent a Data Security Incident. Any audit must be subject to confidentiality and non-disclosure requirements set forth in Section 6 of this Agreement. Utility shall provide ESE with a report of its findings as a result of any audit carried out by or on behalf of Utility. ESE shall, within thirty (30) days, or within a reasonable time period agreed upon in writing between the ESE and Utility, correct any deficiencies identified by Utility, and provide the SOC II audit report or its equivalent or the report produced by the independent auditor to the Utility and provide a report regarding the timing and correction of identified deficiencies to the Utility.
- 10. Investigation.** Upon notice to ESE, ESE shall assist and support Utility in the event of an investigation by any regulator or similar authority, if and to the extent that such investigation relates to Confidential Utility Information Processed by ESE on behalf of Utility. Such assistance shall be at Utility's sole expense, except where such investigation was required due to the acts or omissions of ESE or its Representatives, in which case such assistance shall be at ESE's sole expense.
- 11. Data Security Incidents.** ESE is responsible for any and all Data Security Incidents involving Confidential Utility Information that is Processed by, or on behalf of, ESE. ESE shall notify Utility in writing immediately (and in any event within forty-eight (48) hours) whenever ESE reasonably believes that there has been a Data Security Incident. After providing such notice, ESE will investigate the Data Security Incident, and immediately take all necessary steps to eliminate or contain any exposure of Confidential Utility Information and keep Utility advised of the status of such Data Security Incident and all matters related thereto. ESE further agrees to provide, at ESE's sole cost: (1) reasonable assistance and cooperation requested by Utility and/or Utility's designated representatives, in the

furtherance of any correction, remediation, or investigation of any such Data Security Incident; (2) and/or the mitigation of any damage, including any notification required by law or that Utility may determine appropriate to send to individuals impacted or potentially impacted by the Data Security Incident; and (3) and/or the provision of any credit reporting service required by law or that Utility deems appropriate to provide to such individuals. In addition, within thirty (30) days of confirmation of a Data Security Incident, ESE shall develop and execute a plan, subject to Utility's approval, which approval will not be unreasonably withheld, that reduces the likelihood of a recurrence of such Data Security Incident. ESE agrees that Utility may at its discretion and without penalty immediately suspend performance hereunder and/or terminate the Agreement if a Data Security Incident occurs and it has a reasonable belief of potential ongoing harm. Any suspension made by Utility pursuant to this paragraph 11 will be temporary, lasting until the Data Security Incident has ended, the ESE security has been restored to the reasonable satisfaction of the Utility so that Utility IT systems and Confidential Utility Information are safe and the ESE is capable of maintaining adequate security once electronic communication resumes. Actions made pursuant to this paragraph, including a suspension will be made, or subject to dispute resolution and appeal as applicable, pursuant to the UBP or UBP DERS processes as approved by the Commission.

12. **Cybersecurity Insurance Required.** Commencing by December 1, 2018, ESE shall carry and maintain Cybersecurity insurance in an amount of no less than \$5,000,000 per incident. Utility will maintain at least \$5,000,000 of Cybersecurity insurance.
13. **No Intellectual Property Rights Granted.** Nothing in this Agreement shall be construed as granting or conferring any rights, by license, or otherwise, expressly, implicitly, or otherwise, under any patents, copyrights, trade secrets, or other intellectual property rights of Utility, and ESE shall acquire no ownership interest in the Confidential Utility Information. No rights or obligations other than those expressly stated herein shall be implied from this Agreement.
14. **Additional Obligations.**
  - a. ESE shall not create or maintain data which are derivative of Confidential Utility Information except for the purpose of performing its obligations under this Agreement or as authorized by the UBP or UBP DERS. For purposes of this Agreement, the following shall not be considered Confidential Utility Information or a derivative thereof: (i) any customer contracts, customer invoices, or any other documents created by ESE that reference estimated or actual measured customer usage information, which ESE needs to maintain for any tax, financial reporting or other legitimate business purposes consistent with the UBP or UBP DERS; and (ii) Data collected by ESE from customers through its website or other interactions based on those customers' interest in receiving information from or otherwise engaging with ESE or its partners.

- b. ESE shall comply with all applicable privacy and security laws to which it is subject, including without limitation all applicable Data Protection Requirements and not, by act or omission, place Utility in violation of any privacy or security law known by ESE to be applicable to Utility.
  - c. ESE shall have in place appropriate and reasonable processes and systems, including an Information Security Program, defined as having completed an accepted Attestation as reasonably determined by the Utility in its discretion, to protect the security of Confidential Utility Information and prevent a Data Security Incident, including, without limitation, a breach resulting from or arising out of ESE's internal use, processing, or other transmission of Confidential Utility Information, whether between or among ESE's Third-Party Representatives, subsidiaries and affiliates or any other person or entity acting on behalf of ESE, including without limitation Third-Party Representatives. The Utility's determination is subject to the dispute resolution process under the UBP or UBP DERS.
  - d. ESE and Utility shall safely secure or encrypt during storage and encrypt during transmission all Confidential Information.
  - e. ESE shall establish policies and procedures to provide reasonable and prompt assistance to Utility in responding to any and all requests, complaints, or other communications received from any individual who is or may be the subject of a Data Security Incident involving Confidential Utility Information Processed by ESE to the extent such request, complaint or other communication relates to ESE's Processing of such individual's Confidential Utility Information.
  - f. ESE shall establish policies and procedures to provide all reasonable and prompt assistance to Utility in responding to any and all requests, complaints, or other communications received from any individual, government, government agency, regulatory authority, or other entity that is or may have an interest in the Confidential Utility Information, data theft, or other unauthorized release of Confidential Utility Information, disclosure of Confidential Utility Information, or misuse of Confidential Utility Information to the extent such request, complaint or other communication relates to ESE's accessing or Processing of such Confidential Utility Information.
  - g. ESE will not process Confidential Utility Information outside of the United States or Canada absent a written agreement with Utility. For the avoidance of doubt, Confidential Utility Information stored in the United States or Canada, or other countries as agreed upon in writing will be maintained in a secure fashion at a secure location pursuant to the terms and conditions of this Agreement.
15. **Specific Performance.** The Parties acknowledge that disclosure or misuse of Confidential Utility Information in violation of this Agreement may result in irreparable harm to Utility, the amount of which may be difficult to ascertain and which may not be adequately compensated by monetary damages, and that therefore Utility shall be entitled to specific performance and/or injunctive relief to

enforce compliance with the provisions of this Agreement. Utility's right to such relief shall be in addition to and not to the exclusion of any remedies otherwise available under this Agreement, at law or in equity, including monetary damages, the right to terminate this Agreement for breach and the right to suspend in accordance with the UBP and UBP DERS the provision or Processing of Confidential Utility Information hereunder. ESE agrees to waive any requirement for the securing or posting of any bond or other security in connection with Utility obtaining any such injunctive or other equitable relief.

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

**17. Notices.** With the exception of notices or correspondence relating to potential or pending disclosure under legal compulsion, all notices and other correspondence hereunder shall be sent by first class mail, by personal delivery, or by a nationally recognized courier service. Notices or correspondences relating to potential or pending disclosure under legal compulsion shall be sent by means of Express Mail through the U.S. Postal Service or other nationally recognized courier service which provides for scheduled delivery no later than the business day following the transmittal of the notice or correspondence and which provides for confirmation of delivery. All notices and correspondence shall be in writing and addressed as follows:

If to ESE, to:

ESE Name:  
Name of Contact:  
Address:  
Phone:  
Email:

If to Utility, to:

Utility Name:  
Name of Contact:  
Address:  
Phone:  
Email:

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

- 18. Term and Termination.** This Agreement shall be effective as of the date first set forth above and shall remain in effect until terminated in accordance with the provisions of the service agreement, if any, between the Parties or the UBP or UBP DERS and upon not less than thirty (30) days' prior written notice specifying the effective date of termination, provided, however, that any expiration or termination shall not affect the respective obligations or rights of the Parties arising under this Agreement prior to the effective date of termination. Utility may terminate this Agreement if the ESE is decertified under the UBP or DER UBP, has not served customers for two (2) years, or has not had electronic communication, other than by email, with Utility for one (1) year. Further, Utility may terminate this Agreement immediately upon notice to ESE in the event of a material breach hereof by ESE or its Third-Party Representatives. For the purpose of clarity, a breach of Sections 3-4, 6-11, 13, 14, 16, and 24 shall be a material breach hereof. Upon the expiration or termination hereof, neither ESE nor its Third-Party Representatives shall have any further right to Process Confidential Utility Information or Customer Information and shall immediately comply with its obligations under Section 8 and the Utility shall not have the right to process Confidential ESE Information and shall immediately comply with its obligations under Section 8.
- 19. Consent to Jurisdiction; Selection of Forum.** ESE irrevocably submits to the jurisdiction of the Commission and courts located within the State of New York with regard to any dispute or controversy arising out of or relating to this Agreement. ESE agrees that service of process on it in relation to such jurisdiction may be made by certified or registered mail addressed to ESE at the address for ESE pursuant to Section 11 hereof and that such service shall be deemed sufficient even under circumstances where, apart from this Section, there would be no jurisdictional basis for such service. ESE agrees that service of process on it may also be made in any manner permitted by law. ESE consents to the selection of the New York State and United States courts within \_\_\_\_\_ County, New York as the exclusive forums for any legal or equitable action or proceeding arising out of or relating to this Agreement. If the event involves all of the Utilities jurisdiction will be in Albany County, New York.
- 20. Governing Law.** This Agreement shall be interpreted and the rights and obligations of the Parties determined in accordance with the laws of the State of New York, without recourse to such state's choice of law rules.
- 21. Survival.** The obligations of ESE under this Agreement shall continue for so long as ESE and/or ESE's Third-Party Representatives continue to have access to, are in possession of or acquire Confidential Utility Information even if all Agreements between ESE and Utility have expired or been terminated.
- 22. Counterparts.** This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which shall together constitute

one and the same instrument. Copies of this Agreement and copies of signatures on this Agreement, including any such copies delivered electronically as a .pdf file, shall be treated for all purposes as originals.

23. **Amendments; Waivers.** Except as directed by the Commission, this Agreement may not be amended or modified except if set forth in writing signed by the Party against whom enforcement is sought to be effective. No forbearance by any Party to require performance of any provisions of this Agreement shall constitute or be deemed a waiver of such provision or the right thereafter to enforce it. Any waiver shall be effective only if in writing and signed by an authorized representative of the Party making such waiver and only with respect to the particular event to which it specifically refers.
24. **Assignment.** This Agreement (and the Utility's or ESE's obligations hereunder) may not be assigned by Utility, ESE or Third Party Representatives without the prior written consent of the non-assigning Party, and any purported assignment without such consent shall be void. Consent will not be unreasonably withheld.
25. **Severability.** Any provision of this Agreement which is determined by any court or regulatory body having jurisdiction over this Agreement to be invalid or unenforceable will be ineffective to the extent of such determination without invalidating the remaining provisions of this Agreement or affecting the validity or enforceability of such remaining provisions.
26. **Entire Agreement.** This Agreement (including any Exhibits hereto) constitutes the entire Agreement between the Parties with respect to the subject matter hereof and any prior or contemporaneous oral or written Agreements or understandings with respect to such subject matter are merged herein. This Agreement may not be amended without the written Agreement of the Parties.
27. **No Third-Party Beneficiaries.** This Agreement is solely for the benefit of, and shall be binding solely upon, the Parties and their respective agents, successors, and permitted assigns. This Agreement is not intended to benefit and shall not be for the benefit of any party other than the Parties and the indemnified parties named herein, and no other party shall have any right, claim, or action as a result of this Agreement.
28. **Force Majeure.** No Party shall be liable for any failure to perform its obligations in connection with this Agreement, where such failure results from any act of God or governmental action or order or other cause beyond such Party's reasonable control (including, without limitation, any mechanical, electronic, or communications failure) which prevents such Party from performing under this Agreement and which such Party is unable to prevent or overcome after the exercise of reasonable diligence. For the avoidance of doubt a Data Security Incident is not a force majeure event.
29. **Relationship of the Parties.** Utility and ESE expressly agree they are acting as independent contractors and under no circumstances shall any of the employees

of one Party be deemed the employees of the other for any purpose. Except as expressly authorized herein, this Agreement shall not be construed as authority for either Party to act for the other Party in any agency or other capacity, or to make commitments of any kind for the account of or on behalf of the other.

30. **Construction.** This Agreement shall be construed as to its fair meaning and not strictly for or against any party.
31. **Binding Effect.** No portion of this Agreement is binding upon a Party until it is executed on behalf of that Party in the space provided below and delivered to the other Party. Prior to such execution and delivery, neither the submission, exchange, return, discussion, nor the negotiation of this document, whether or not this document is then designated as a "draft" document, shall have any binding effect on a Party.

*[signature page follows]*

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

**UTILITY**

**ESE**

By: \_\_\_\_\_

By: \_\_\_\_\_

Name: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_



## SELF-ATTESTATION OF INFORMATION SECURITY CONTROLS

Each Utility, for itself only, represents that for all information received from Third Party in response or pursuant to this Self-Attestation that is marked CONFIDENTIAL by Third Party (Confidential Self-Attestation Information) Utility shall: (A) hold such Confidential Self-Attestation Information in strict confidence; (B) not disclose such Confidential Self-Attestation Information to any other person or entity; (C) not Process such Confidential Self-Attestation Information outside of the United States or Canada; (D) not Process such Confidential Self-Attestation Information for any purpose other than to assess the adequate security of Third party pursuant to this Self-Attestation and to work with Third party to permit it to achieve adequate security if it has not already done so; (E) limit reproduction of such Confidential Self-Attestation Information; (F) store such Confidential Self-Attestation Information in a secure fashion at a secure location in the United States or Canada that is not accessible to any person or entity not authorized to receive such Confidential Self-Attestation Information under the provisions hereof; (G) otherwise use at least the same degree of care to avoid publication or dissemination of such Confidential Self-Attestation Information as Utility employs (or would employ) with respect to its own confidential information that it does not (or would not) desire to have published or disseminated, but in no event less than reasonable care.

The Requirements to complete the Self-Attestation are as follows (check all that apply to Third Party's computing environment, leave blank all that do not apply to Third Party's computing environment. For items that do not apply. If there are plans to address items that do not currently apply within the next 12 months, place an asterisk in the blank and the month/year the requirement is projected to apply to the Third Party's computing environment), comments regarding plans for compliance are encouraged:

This SELF-ATTESTATION OF INFORMATION SECURITY CONTROLS (“Attestation”), is made as of this \_\_\_\_ day of \_\_\_\_\_, 20\_\_ by \_\_\_\_\_, a third party (“Third Party”) to Consolidated Edison Company of New York, Inc., Orange and Rockland Utilities, Inc., Central Hudson Gas & Electric Corporation, National Fuel Gas Distribution Corporation, The Brooklyn Union Gas Company d/b/a National Grid NY, KeySpan Gas East Corporation d/b/a National Grid, and Niagara Mohawk Power Corporation d/b/a National Grid, New York State Electric & Gas Corporation and Rochester Gas and Electric Corporation (together, the New York State Joint Utilities or “JU”).

WHEREAS, Third Party desires to retain access to certain Confidential Utility Information<sup>1</sup> (as defined in this Data Security Agreement), Third Party must THEREFORE self-attest to Third Party's compliance with the Information Security Control Requirements ("Requirements") as listed herein. Third Party acknowledges that non-compliance with any of the Requirements may result in the termination of utility data access as per the discretion of any of the JU, individually as a Utility or collectively, in whole or part, for its or their system(s). Any termination process will proceed pursuant to the Uniform Business Practices or Distributed Energy Resources Uniform Business Practices.

- \_\_\_\_\_ An Information Security Policy is implemented across the Third Party corporation which includes officer level approval.
- \_\_\_\_\_ An Incident Response Procedure is implemented that includes notification within 48 hours of knowledge of a potential incident alerting utilities when Confidential Utility Information is potentially exposed, or of any other potential security breach.
- \_\_\_\_\_ Role-based access controls are used to restrict system access to authorized users and limited on a need-to-know basis.
- \_\_\_\_\_ Multi-factor authentication is used for all remote administrative access, including, but not limited to, access to production environments.
- \_\_\_\_\_ All production systems are properly maintained and updated to include security patches on a periodic basis. Where a critical alert is raised, time is of the essence, and patches will be applied as soon as practicable.
- \_\_\_\_\_ Antivirus software is installed on all servers and workstations and is maintained with up-to-date signatures.
- \_\_\_\_\_ All Confidential Utility Information is encrypted in transit utilizing industry best practice encryption methods.
- \_\_\_\_\_ All Confidential Utility Information is secured or encrypted at rest utilizing industry best practice encryption methods, or is otherwise physically secured.

---

<sup>1</sup> "Confidential Utility Information" means, collectively, aggregated and customer -specific information that Utility is: (A) required by the Uniform Business Practices ("UBP") at Section 4: Customer information(C)(2), (3) or Distributed Energy Provider ("DER") UBP at Section 2C: Customer data, to provide to ESCO, Direct Customer or DER Supplier and or (B) any other Data provided to ESE by Utility and marked confidential by the Utility at the time of disclosure, or (C) a Utility's operations and/or systems, including but not limited to log-in credentials, but excludes (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; (iv) information which was independently developed by the Receiving Party or its Representatives without reference to, or consideration of, the Confidential Information; or (v) information provided by the customer with customer consent where the customer expressly agrees that the information is public.

\_\_\_\_\_ It is prohibited to store Confidential Utility Information on any mobile forms of storage media, including, but not limited to, laptop PCs, mobile phones, portable backup storage media, and external hard drives, unless the storage media or data is encrypted.

\_\_\_\_\_ All Confidential Utility Information is stored in the United States or Canada only, including, but not limited to, cloud storage environments and data management services.

\_\_\_\_\_ Third Party monitors and alerts their network for anomalous cyber activity on a 24/7 basis.

\_\_\_\_\_ Security awareness training is provided to all personnel with access to Confidential Utility Information.

\_\_\_\_\_ Employee background screening occurs prior to the granting of access to Confidential Utility Information.

\_\_\_\_\_ Replication of Confidential Utility Information to non-company assets, systems, or locations is prohibited.

\_\_\_\_\_ Access to Confidential Utility Information is revoked when no longer required, or if employees separate from the Third Party.

Additionally, the attestation of the following item is requested, but is NOT part of the Requirements:

\_\_\_\_\_ Third Party maintains an up-to-date SOC II Type 2 Audit Report, or other security controls audit report.

IN WITNESS WHEREOF, Third Party has delivered accurate information for this Attestation as of the date first above written.

Signature: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

**THIRD-PARTY REPRESENTATIVE AGREEMENT**

This Third-Party Agreement to be provided to the Utility upon request.

I, \_\_\_\_\_, have read the Agreement between \_\_\_\_\_, (“Company”) and \_\_\_\_\_, (“Utility”) 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 Utility to the ESE pursuant to the Agreement.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date