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[1] (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.

[1] "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: _____