DATA SECURITY AGREEMENT

This Data Security Agreement ("Agreement") effective _____ is made and entered into this _____ day of _____, 2023 by and between National Fuel Gas Distribution Corporation, 6363 Main Street, Williamsville, NY 14221 ("Company") and _____, an Energy Service Entity ("ESE"), with offices at _____; and together with Company the ("Parties" and each, individually, a "Party").

RECITALS

WHEREAS, ESE desires to have access to certain Company customer information, either customer-specific or aggregated customer information, the Company is obligated to provide information under 52 Pa. Code § 62.76 and/or the Pennsylvania Public Utility Commission ("Commission") has ordered Company to provide to ESE customer information; and

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

WHEREAS, Natural Gas Supplier ("NGS"), may utilize a third party to fulfill its Service obligations, including but not limited to, Electronic Data Interchange ("EDI") communications with Company, schedule gas supplies for DMT Service Customer(s), DMLMT Service Customer(s), MMT Customer(s) and/or SATC Customer(s) via Company's Transportation Scheduling System ("TSS") and/or access Confidential Information via Company issued accounts/passwords; and

WHEREAS, a DMT Service Customer, DMLMT Service Customer or MMT Customer (individually, "Standalone Customer") may schedule its own gas supplies via Company's TSS without an NGS; and

WHEREAS, a Standalone Customer with daily metering and communications equipment which enable the Company to obtain each day meter readings of the volume of gas delivered to the Company for the Customer's account and the volume of gas from the Company used by the Customer each day may access to such information via Company issued accounts/passwords; and

WHEREAS, NGS or Standalone Customer utilization of a third party provider does not relieve NGS or Standalone Customer of their transactional obligation such that they must ensure that the third party provider must comply with all NGS or Standalone Customer obligations; and

WHEREAS, Company 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 Company; 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 52 PA Code §§ 59.91-59.99 or Governing Documents to receive from the end use customer and provide to the Company to enroll the customer or (B) any other information provided by ESE to Company 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 the Party receiving the information from the other Party hereto ("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 the Party disclosing the information ("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 Company Information" means information that Company is: (A) required by 52 Pa. Code § 62.76 to provide to NGS or Standalone Customer and which ESE does obtain from Company or (B) any other information provided to ESE by Company and marked confidential by the Company 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 Company 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 Company 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) Commission rules, regulations, and guidelines relating to confidential customer data. Subject to the above, ESE will determine and implement the necessary Data Protection Requirements to be in compliance with the Governing Documents.

e. "Data Security Incident" means a situation when Company 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, computer systems, network and devices used by the ESE and/or its Third Party Representatives' business for Processing hereunder; (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. "Customer Agent" is a third party that has access to Confidential Information via Company issued accounts/passwords and/or schedules gas on behalf of a NGS. Customer Agent includes, but is not limited to, third party Brokers Non-selling marketer and Nontraditional marketer as defined 52 PA Code §62.101 that access Confidential Information via Company issued accounts/passwords."

g. "Standalone Customer" is a customer eligible for natural gas transportation service under 52 PA Code § 60.3 defined in Company's Tariff as a DMT Service Customer, DMLMT Service Customer or MMT Customer, that schedules its own gas supplies via Company's TSS without an NGS.

h. "NGS" has the meaning set forth in 52 PA Code § 62.72 and as it may be amended from time to time, which is "An entity other than an NGDC, but including NGDC marketing affiliates, which provides natural gas supply services to retail gas customers utilizing the jurisdictional facilities of an NGDC."

i. "ESE" shall have the meaning set forth in the Recitals and for the avoidance of doubt, includes but is not limited to NGSs or Standalone Customers, Customer Agents and contractors of such entities with which Company electronically exchanges data other than by email and any other entities with which Company electronically exchanges data other than by email or by a publicly available portal.

j. "PUC" 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 Company 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, including Customer Agents, acting on behalf of NGSs or Standalone Customers, that are contractors or subcontractors and that store, transmit or process Confidential Company 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 Company Information for the purposes of providing Services.

m. “Services” mean any assistance in the competitive markets provided by ESEs to end use customers or NGSs or Standalone Customers that also require interaction with a Company, including but not limited to the electronic exchange of information with a Company, and must be provided in accordance with the Governing Documents where applicable. Governing Documents may not apply to Third Party Representatives that are not electronically interconnected with Company other than by email.

n. “Company Data” means data held by Company, whether produced in the normal course of business or at the request of ESE.

o. “Tariff” means (Gas--Pa. P.U.C. No. 9 or any superseding tariff).

p. “DMT Service Customer” means, unless redefined in any superseding tariff, any entity that has executed a DMT Service Agreement with the Company for transportation of gas by the Company under Tariff Rate Schedule For Daily Metered Transportation Service.

q. “DMLMT Service Customer” means, unless redefined in any superseding tariff, any entity that has executed a DMLMT Service Agreement with the Company for transportation of gas by the Company under Tariff Rate Schedule For Daily Metered Transportation Service.

r. “MMT Customer” means, unless redefined in any superseding tariff, a customer that receives transportation service from the Company under this rate schedule and receives gas supply from a Monthly Metered Natural Gas Supplier.

s. “SATC Customer” means, unless redefined in any superseding tariff, a customer that has enrolled to receive gas supply service from a qualified supplier under the Company’s Small Aggregation Transportation Supplier Service.

2. Scope of the Agreement. This Agreement shall govern security practices of ESEs that electronically receive or exchange Confidential Company Information, other than by email, with the Company IT Systems and security practices that apply to all Confidential Company Information disclosed to ESE or to which ESE is given access by Company, including all archival or back- up copies of the Confidential Company 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 Company, ESE or Company will immediately notify the Company/ESE and destroy any such information in the appropriate manner.

3. **ESE Compliance with all Applicable Regulatory Requirements.** The Parties agree that 52 PA Code §§ 62.71-62.81, Company's Tariff and Commission Orders, rules and regulations set forth rules governing the protection of Confidential Information (collectively, "Governing Documents") and electronic exchange of information between the Parties, including but not limited to electronic data interchange ("EDI").

4. **Customer Consent.** The Parties agree that the Governing Documents govern an ESE's obligation to obtain informed consent from all customers about whom ESE requests Confidential Company Information from Company. The ESE agrees to comply with the Governing Documents regarding customer consent.

5. **Provision of Information.** Company agrees to provide to ESE or its Representatives, certain Confidential Company Information, as requested, provided that: (A) ESE and its Representatives with an electronic connection to Company other than by email are in compliance with the terms of this Agreement in all material respects; (B) if required by Company due to the identification of a suspected or actual Data Security Incident, ESE shall undergo an audit, at the ESE's expense[1]; (C) ESE (and its Third-Party Representatives with an electronic connection to the Company other than by email) shall have and maintain throughout the term, systems and processes in place and as detailed in the Self Attestation to protect Company IT systems, data privacy protections and Confidential Company Information. Provided the foregoing prerequisites have been satisfied, ESE shall be permitted access to Confidential Company Information and/or Company shall provide such Confidential Company Information to ESE. Notwithstanding the foregoing, a suspected or actual Data Security Incident will not be the basis for the refusal of Company to provide ESE with Company Confidential Information or the undertaking of the audit referenced in this Section B if, i) ESE provides a written verification to the Company that a suspected Data Security Incident was not confirmed and did not result in an actual Data Security Incident, or ii) ESE provides a written verification to the Company that an actual Data Security Incident has been resolved and appropriate controls have been implemented by the ESE to protect Company's IT Systems and Company Confidential Information; provided that ESE's actions and written verifications thereof are satisfactory to the Company and are subject to review and approval by Company, which approval shall not be unreasonably withheld or delayed. For avoidance of doubt, the foregoing does not prevent Company's rights to immediately suspend ESE's access to Company Confidential Information in response to a suspected or actual Data Security Incident in accordance with the terms of this Agreement. 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

[1] An audit related to a Data Security Incident is used to verify that the necessary Information Security Control Requirements set forth in Exhibit A are in place for the Company to provide certain Confidential Company Information to the ESE or its Third-Party Representatives with an electronic connection to the utility, other than by email. The same audit requirements will apply as in Section 9. However, the ESE will be responsible for the cost of the audit in order to be re-authorized to receive data from the Company.

assert any lien over or right to withhold from the other Party any Data and/or Confidential Information of the other Party. Company will comply with the security requirements set forth in Exhibit A with respect to its systems that Process or contain Confidential ESE Information and to the extent such mandates do not conflict with other legal requirements.

6. Confidentiality. ESE shall: (A) hold all Confidential Company Information in strict confidence pursuant to the Governing Documents; except as otherwise expressly permitted by Section 7 herein; (B) not disclose Confidential Company Information to any Third-Party Representatives, or affiliates, except as set forth in Section 7(a) of this Agreement; (C) not Process Confidential Company Information other than for the Services defined in the Recitals as authorized by this Agreement; (D) limit reproduction of Confidential Company Information; (E) store Confidential Company Information in a secure fashion at a secure location that is not accessible to any person or entity not authorized to receive the Confidential Company Information under the provisions hereof; and (F) otherwise use at least the same degree of care to avoid publication or dissemination of the Confidential Company 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. At all times, Company shall have the right for cause to request reasonable further assurances that the foregoing restrictions and protections concerning Confidential Company Information are being observed and ESE shall be obligated to promptly provide Company with the requested assurances. An ESE may provide Confidential Company Information to a Third-Party representative without a direct electronic connection with the Utility, to assist the ESE in providing permitted Services, but an ESE utilizing such Third party Representative shall be solely responsible and fully liable for the actions of the Third Party Representative.

Company 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; and (F) otherwise use at least the same degree of care to avoid publication or dissemination of the Confidential ESE Information as Company 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. 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 Company 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 Company 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 Governing Documents, provided that each such Third-Party Representative is advised by the disclosing Party of the sensitive and confidential nature of such Confidential Information. Notwithstanding the foregoing, the ESE shall be liable for any act or omission of its 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 Company's written demand in accordance with this Section 8, ESE shall (and shall cause its Third-Party Representatives to), subject to applicable federal, state and local laws, rules, regulations and orders, cease to access and Process Confidential Company Information and shall at the Company's option: (A) return such Confidential Company Information to Company in such manner, format, and timeframe as reasonably requested by Company or, if not so directed by Company, (B) shred, permanently erase and delete, degauss or otherwise modify so as to make unreadable, unreconstructible and indecipherable ("Destroy") all copies of all Confidential Company Information (including any and all extracts, compilations, studies, or other documents based upon, derived from, or containing Confidential Company

Information) that has come into ESE's or its Third-Party Representatives' possession, including Destroying Confidential Company 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 Company Information by ESE and its Third-Party Representatives shall cease provided any items, including Confidential Company Information 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. Company, when making a written demand of ESE for the return or destruction of Confidential Company Information will specify the reason for the demand. ESE agrees that upon a customer revocation of consent, ESE warrants that it will no longer access through Company such Customer's Confidential Company Information. Notwithstanding the foregoing, ESE and its Third-Party Representatives shall not be obligated to erase Confidential Company 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 Company Information from such computer backup system and; (3) keep all such Confidential Company Information confidential in accordance with this Agreement. ESE shall, upon request, certify to Company 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 Company 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 Company Information pursuant to this Section may occur if the ESE has been decertified pursuant to the Governing Documents, the Company has been notified of a suspected or actual Data Security Incident and Company has a reasonable belief of potential ongoing harm to Company's IT Systems, or the Confidential Company Information has been held for a period in excess of its retention period as required by any applicable law, rule, regulation or order. Notwithstanding the foregoing, an ESE will not be obligated to return or Destroy Confidential Company Information due to a suspected or actual Data Security Incident if ESE provides a written verification to the Company within 30 day period set forth above that i) a suspected Data Security Incident was not confirmed and did not result in an actual Data Security Incident, or ii) that the actual Data Security Incident has been resolved and appropriate controls have been implemented by the ESE to protect Company's IT Systems and Company Confidential Information; provided that ESE's actions and written verifications thereof are satisfactory to the Company and are subject to review and approval by Company, which approval shall not be unreasonably withheld or delayed. 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 Company, Company will Destroy or return, at ESE's option, Confidential ESE Information.

9. **Audit.** Upon thirty (30) days' written notice to ESE, ESE shall permit a reputable third party auditor selected by the Company through a competitive solicitation and agreed to by the ESE, such agreement not to be unreasonably withheld, (the "CSA") to audit and inspect ESE, at Company'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 Company's regulators).The audit may include (A) the facilities of ESE and ESE's Third-Party Representatives where Confidential Company Information is Processed by or on behalf of ESE; (B) any computerized or paper systems used to Process Confidential Company 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 Company 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 Company, or commits to complete an independent third-party audit of ESE's compliance with this Agreement acceptable to the Company at ESE's sole expense, within one hundred eighty (180) days, no audit by a third party auditor selected by the Company through a CSA and conducted at Company's sole expense is necessary absent a Data Security Incident. Notwithstanding the foregoing, a suspected or actual Data Security Incident will not be the basis for an audit hereunder if, i) ESE provides a written verification to the Company that the suspected Data Security Incident was not confirmed and did not result in an actual Data Security Incident, or ii) ESE provides a written verification to the Company that the actual Data Security Incident has been resolved and appropriate controls have been implemented by the ESE to protect Company's IT Systems and Company Confidential Information; provided that ESE's actions and written verifications thereof are satisfactory to the Company and are subject to approval by Company, which approval shall not be unreasonably withheld or delayed. In the event an audit relating to a Data Security Incident does occur, the scope will be to investigate ESE's IT Systems and security practices involved in the Data Security Incident; provided that Company has the right to approve the scope of the audit, with such approval not to be unreasonably withheld or delayed. Any audit must be subject to confidentiality and non-disclosure requirements set forth in Section 6 of this Agreement; provided that any information obtained by Company and/or its auditors which is not capable of being marked confidential, shall be deemed to be ESE Confidential Information; provided further, however, that Company shall be permitted to share Confidential Information as contemplated in Section 7 of this Data Security Agreement and to use Confidential Information in order to pursue appropriate remedial and/or legal actions that flow from a Data Security Incident consistent with an appropriate protective order. The auditor will audit the ESE's compliance with the Agreement and provide those results to the Company and ESE. The audit report sent to the Company shall not include any ESE confidential information, it will simply provide an assessment as to the ESE's compliance with the terms of this Agreement. In the event of a "failed" audit dispute, the dispute resolution processes outlined in the Governing Documents can be utilized or a complaint can be brought to the Commission. Company shall provide ESE with a report of the findings as a result of any audit carried out by an auditor selected

through the CSA. ESE shall, within ninety (90) days, or within a reasonable time period agreed upon in writing between the ESE and Company, correct any deficiencies identified in the audit report. In the event ESE elects (as set forth above) to have an independent third-party conduct an audit of ESE's compliance with this Agreement or elects to undergo a SOC II audit, ESE shall provide the SOC II report or its equivalent or the report produced by ESE's independent auditor to the Company and provide a report regarding the timing and correction of identified deficiencies, if any, to the Company.

10. Investigation. Upon notice to ESE, ESE shall assist and support Company in the event of an investigation by any regulator or similar authority, if and to the extent that such investigation relates to Confidential Company Information processed by ESE on behalf of Company. Such assistance shall be at Company'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 Company Information that is Processed by, or on behalf of, ESE. ESE shall notify Company 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 Company Information and keep Company 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 Company and/or Company'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 Company 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 Company 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 Company's approval, which approval will not be unreasonably withheld or delayed, that reduces the likelihood of a recurrence of such Data Security Incident. ESE agrees that Company may at its reasonable 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. Notwithstanding the foregoing, a Data Security Incident will not be the basis for ongoing suspension and/or a termination if, based on ESE's investigation hereunder, ESE provides a written verification to the Company that the Data Security Incident has been resolved and appropriate controls have been implemented by the ESE to protect Company's IT Systems or an ongoing loss of Company Confidential Information; provided that ESE's actions and written verifications thereof are satisfactory to the Company and subject to review and approval by Company, which approval shall not be unreasonably withheld or delayed. For avoidance of doubt, the foregoing does not prevent Company's rights

to immediately suspend ESE's access to Company Confidential Information in response to a suspected or actual Data Security Incident in accordance with the terms of this Agreement until the foregoing determinations and verifications are completed to the satisfaction of the Company. Any suspension made by Company 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 Company so that Company IT systems and Confidential Company Information are safe and the ESE is capable of maintaining adequate security once electronic communication resumes. During any suspension under this Agreement, Company agrees to take reasonable steps to allow ESE to continue to enroll and service customers, so long as the Company can verify that the Confidential Information contained in the Company's IT Systems can be maintained as secure. Actions made pursuant to this paragraph, including a suspension will be made, or subject to dispute resolution and appeal as applicable, pursuant to the Governing Documents processes as approved by the Commission.

12. Cybersecurity Insurance Required. ESE shall carry and maintain Cybersecurity insurance in an amount of no less than $2,000,000 per incident. Company will maintain at least $2,000,000 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 Company, and ESE shall acquire no ownership interest in the Confidential Company 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 Company Information except for the purpose of performing its obligations under this Agreement or as authorized by the Governing Documents or as expressly authorized by the customer, unless that use violates Federal, State, or local laws, tariffs, rules and/or regulations. For purposes of this Agreement, the following shall not be considered Confidential Company 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 Governing Documents; 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 Company in violation of any privacy or security law known by ESE to be applicable to Company.

c. ESE shall have in place appropriate and reasonable processes and systems,

including an Information Security Program, defined as having completed an accepted Self-Attestation attached hereto as Exhibit A (or in a subsequent form filed by Company in a tariff supplement for Commission review and approval), to protect the security of Confidential Company Information and protect against 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 Company 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 Company's determination is subject to the dispute resolution process under the Governing Documents. In the event the Company and ESE are unable to resolve the dispute by mutual agreement within thirty (30) days of said referral, the dispute shall be referred for mediation through the Commission's Office of Administrative Law Judge. A party may request mediation prior to that time if it appears that informal resolution is not productive.

d. ESE and Company shall safely secure or encrypt during storage and encrypt during transmission all Confidential Information, except that no encryption in transit is required for email communications.

e. ESE shall establish policies and procedures to provide reasonable and prompt assistance to Company 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 Company Information Processed by ESE to the extent such request, complaint or other communication relates to ESE's Processing of such individual's Confidential Company Information.

f. ESE shall establish policies and procedures to provide all reasonable and prompt assistance to Company 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 Company Information, data theft, or other unauthorized release of Confidential Company Information, unauthorized disclosure of Confidential Company Information, or misuse of Confidential Company Information to the extent such request, complaint or other communication relates to ESE's accessing or Processing of such Confidential Company Information.

g. ESE will not process Confidential Company Information outside of the United States or Canada absent a written agreement with Company. For the avoidance of doubt, Confidential Company 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.

h. Any modifications to the DSA or SA will be submitted to the Pennsylvania Public Utility Commission for approval prior to implementation.

15. **Specific Performance.** The Parties acknowledge that disclosure or misuse of Confidential Company Information in violation of this Agreement may result in irreparable harm to Company, the amount of which may be difficult to ascertain and which may not be adequately compensated by monetary damages, and that therefore Company shall be entitled to specific performance and/or injunctive relief to enforce compliance with the provisions of this Agreement. Company's right to such relief shall be in addition to and not to the exclusion of any remedies otherwise available under this Agreement, at law or in equity, including monetary damages, the right to terminate this Agreement for breach and the right to suspend the provision or Processing of Confidential Company Information under the Governing Documents. ESE agrees to waive any requirement for the securing or posting of any bond or other security in connection with Company obtaining any such injunctive or other equitable relief.

16. **Indemnification.** To the fullest extent permitted by law, ESE shall indemnify and hold Company, 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 Company.

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 Company, to:

Company Name: National Fuel Gas Distribution Corporation

Name of Contact:	Rates and Regulatory Affairs Department
Address:	6363 Main Street, Williamsville, NY 14221
Phone:	716-857-6824
Email:	NFGratesPAD@natfuel.com

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

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 Governing Documents 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. Company may terminate this Agreement if the ESE loses its status as a Licensed Supplier, has not served customers for two (2) years. Further, Company 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, 6-10, 13, 14, 16, and 24 shall be a material breach hereof, but subject to ESE's right to cure any such breach within 15 days of notice of such breach. Prior to providing notice of a termination of the Agreement due a Data Security Incident, ESE and Company shall work in good faith for a reasonable time period as determined by the Company to investigate and evaluate the incident in accordance with Section 11. For avoidance of doubt, the foregoing does not prevent Company's rights to immediately suspend ESE's access to Company Confidential Information in response to the Data Security Incident in accordance with the terms of this Agreement. The Breaching Party will provide the non-breaching Party with a written description and notice of the material breach. Upon the expiration or termination hereof, neither ESE nor its Third-Party Representatives shall have any further right to Process Confidential Company Information, unless the customer has given written or electronic consent to do so, and shall immediately comply with its obligations under Section 8 and the Company shall not have the right to process Confidential ESE Information and shall immediately comply with its obligations under Section 8. In the event of a dispute relating to actions pursuant to this Agreement, the dispute resolution processes outlined in the Governing Documents can be utilized or a complaint can be brought to the Commission; provided, however, that the Company will not be required to obtain a Commission Order prior to suspending access to Company Confidential Information in the event of a suspected or actual Data Security Incident.

19. Consent to Jurisdiction; Selection of Forum. ESE and Company irrevocably submit to the jurisdiction of the Commission and courts located within the Commonwealth of Pennsylvania with regard to any dispute or controversy arising out of or relating to this Agreement. ESE and Company agree that service of process on it in relation to such jurisdiction may be made by certified or registered mail addressed to ESE/Company at the address for ESE/Company 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 and Company agree that service of process on it may also be made in any manner permitted by law. ESE and Company consent to the selection of the Pennsylvania and United States courts within Erie County, Pennsylvania as the exclusive forums for any legal or equitable action or proceeding arising out of or relating to this Agreement. Notwithstanding the foregoing, Company and ESE may mutually agree to a different forum for any legal or equitable action or proceeding arising out of or relating to this Agreement.

20. Governing Law. This Agreement shall be interpreted, and the rights and obligations of the Parties determined in accordance with the laws of the Commonwealth of Pennsylvania, 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 Company Information even if all Agreements between ESE and Company 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 Company's or ESE's obligations hereunder) may not be assigned by Company, 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 superseded hereby, including all Data Security Agreements between ESE and the Company that were executed prior to the effective date of this Agreement. 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.** Company 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. Each Party agrees that this Agreement and any other documents to be delivered in connection herewith may be electronically signed, and that any electronic signatures appearing on this Agreement or such other document are the same as handwritten signatures for the purposes of validity, enforceability, and admissibility. 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.

NATIONAL FUEL GAS DISTRIBUTION CORPORATION

By: _____ By: _____

Name: _____ Name: _____

Title: _____ Title: _____

EXHIBIT A

SELF-ATTESTATION
OF INFORMATION SECURITY CONTROLS

National Fuel Gas Distribution Corporation ("Company") represents that for all information received from ESE or its Third Party Representatives in response or pursuant to this Self-Attestation that is marked CONFIDENTIAL by ESE or its Third Party Representatives and data or information that is not capable of being marked as confidential, provided however that Company shall be permitted to share information as permitted in Section 7 of the Data Security Agreement and to use Confidential Information in order to pursue appropriate remedial and/or legal actions that flow from a Data Security Incident consistent with an appropriate protective order, (Confidential Self-Attestation Information). Company 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 ESE or its Third Party Representatives pursuant to this Self-Attestation and to work with ESE or its Third Party Representatives 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 Company 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 ESE's computing environment, leave blank all that do not apply to ESE'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 ESE'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_____, 2023 by _____, an ESE.

WHEREAS, ESE desires to retain access to certain Confidential Company Information[1] (as defined in this Data Security Agreement), ESE must THEREFORE self- attest to ESE's compliance with the Information Security Control Requirements ("Requirements") as listed herein. Subject to the terms of the Data Security Agreement, which includes without limitation use of the dispute resolution processes set forth in the Governing Documents, ESE acknowledges that non-compliance with any of the Requirements may result in the termination of Company data access, subject to the terms of the Data Security Agreement and 30 days' advance notice to ESE, citing the reasons therefor. Any termination process will proceed pursuant to the Governing Documents.

_____ An Information Security Policy is implemented across the ESE corporation which includes officer level approval.

_____ An Incident Response Procedure is implemented that includes notification within 48 hours of knowledge of a suspected incident, alerting utilities, if required pursuant to the Data Security Agreement, when Confidential Company Information is potentially exposed, or of any other suspected 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.

_____ All production systems are properly maintained and updated to include security patches on a regular 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 supported servers and workstations and is maintained to a supported release. If a pattern based antivirus solution is utilized, pattern signatures are to be kept up-to-date.

_____ All Confidential Company Information is encrypted in transit utilizing industry best practice encryption methods, except that Confidential Information does not need to be encrypted during email communications.

[1] "Confidential Company Information" means, information that Company is: (A) required by 52 Pa. Code § 62.76 to provide to ESE and which ESE does obtain from Company or (B) any other Data provided to ESE by Company and marked confidential by the Company 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.

_____ All Confidential Company Information is secured or encrypted at rest utilizing industry best practice encryption methods, or is otherwise physically secured.

_____ It is prohibited to store Confidential Company 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 Company Information is stored in the United States or Canada only, including, but not limited to, cloud storage environments and data management services.

_____ ESE 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 Company Information.

_____ Employee background screening occurs prior to the granting of access to Confidential Company Information.

_____ Replication of Confidential Company Information to non-company assets, systems, or locations is prohibited, except to Third Party Representatives subject to the terms of the Agreement.

_____ Access to Confidential Company Information is revoked when no longer required, or if employees separate from the ESE or Third Party Representative.

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

_____ ESE maintains an up-to-date SOC II Type 2 Audit Report, or other security controls audit report.

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

Signature: _____

Name: _____

Title: _____

Date: _____