NONDISCLOSURE AGREEMENT WITH DATA SECURITY REQUIREMENTS

This Nondisclosure Agreement (the "***Agreement***") is made as of the 30th day of January, 2024 ("Effective Date") by and between The United Illuminating Company, a Connecticut corporation with offices at 100 Marsh Hill Road, Orange, CT 06477 and its subcontractors (if applicable) ("***UI***"), Eversource Energy Service Company, a Connecticut corporation with offices at 107 Selden Street, Berlin, CT 06037 and its subcontractors (if applicable) ("***Eversource***") , and <Contractor Name> and its subcontractors (if applicable) ("***Receiving Party***") UI/Eversource and having an office at <Contractor's Headquarter Location>, (collectively the "***Parties***") to assure the protection of the confidential or proprietary nature of information to be disclosed or made available to Receiving Party by UI/Eversource for the Purpose set forth herein. All proposals are subject to be submitted to the Public Utilities Regulatory Authority ("PURA") or PURA's Process Monitor selected in PURA Docket No. 24-08-08, Non-Wires Solutions Process Initiation Phase ("NV5") or PURA. Prior to submitting their proposal to UI/Eversource, the Receiving Party is responsible for ensuring appropriate confidentiality protections are in place with the Process Monitor or PURA to prevent unauthorized or public disclosure of any Confidential Information.

WHEREAS, Receiving Party has submitted a response to, or plans to submit a response to, a specific distribution need provided by UI/Eversource under its annual Grid Needs Filing per the Non-Wires Solutions ("NWS") process per Final Decision ("Decision") of the PURA in Docket No. 17-12-03RE07 ("***Subject Activities***"); and

WHEREAS, in connection with such Subject Activities, UI/Eversource shall make available to Receiving Party certain information regarding their electric system to help support the competitive solicitation issued by UI/Eversource, and any other relevant business confidential information all of which information UI/Eversource consider proprietary or confidential (hereinafter the "***Confidential Information***"); and

WHEREAS, UI/Eversource have concluded that it is in their best interest to disclose or make available such Confidential Information to Receiving Party pursuant to all of the terms and conditions set forth herein so that Receiving Party can be compliant with the Receiving Party's role established by PURA's Decision ("***Purpose***"); and

WHEREAS, UI/Eversource's disclosure of Confidential Information and Receiving Party's use of the Confidential Information is conditioned entirely on the Parties' entering into and compliance with this Agreement in order to protect UI/Eversource's Confidential Information and limit its disclosure and use solely to the Receiving Party and for the Purpose set forth herein.

NOW, THEREFORE, in consideration of the mutual understandings of the parties, it is agreed as follows:

1) Definitions.

a) "Confidential Information" as used in this Agreement means the Confidential Information expressly described above and any and all information that is designated or otherwise identified orally or in writing as confidential or proprietary or which, under the circumstances surrounding disclosure, Receiving Party should know is treated as confidential by UI/Eversource. Confidential Information expressly includes Critical Energy Infrastructure Information and Personal Data (defined below). Confidential Information includes but is not limited to notes, documents, memoranda or other writings including electronic writings, including any materials which copy or disclose Confidential Information, prepared by Receiving Party based on information contained in the Confidential Information. Receiving Party shall treat the Confidential Information in strict confidence and with the same degree of care that it accords to its own confidential information but in no event less than a reasonable degree of care. Without limiting the generality of the foregoing, all Confidential Information received by Receiving Party pursuant to this Agreement shall be maintained in a secure place and access to the Confidential Information shall be restricted solely to Receiving Party.

b) "Critical Energy Infrastructure Information" means engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure (physical or virtual) that (A) relates details about the production, generation, transmission, or distribution of energy; (B) could be useful to a person planning an attack on critical infrastructure; (C) is exempt from mandatory disclosure under the Freedom of Information Act; and (D) gives strategic information beyond the location of the critical infrastructure.

c) "Personal Data" means any information about an individual, including an employee, vendor, customer, or potential customer of UI/Eversource or their affiliates, including, without limitation: (A) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, biometric records, personal electronic mail address, internet identification name, network password or internet password; (B) information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household, or (C) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information, as well as cookie information and usage and traffic data or profiles, that is combined with any of the foregoing.

d) "Data Security Incident" means: (A) the loss or misuse (by any means) of Confidential Information; (B) the inadvertent, unauthorized and/or unlawful Processing, corruption, modification, transfer, sale or rental of Confidential Information; (C) any other act, omission or circumstance that compromises or may reasonably compromise the security, confidentiality, or integrity of Confidential Information, including but not limited to incidents where Confidential Information has been damaged, lost, corrupted, destroyed, or accessed, acquired, modified, used, or disclosed by any unauthorized person, by any person in an unauthorized manner, or for an unauthorized purpose; (D) any act, omission or circumstance that compromises or may reasonably compromise the cybersecurity of the products and services provided to UI/Eversource by Receiving Party or the physical,

technical, administrative, or organizational safeguards protecting Receiving Party's systems or, if Receiving Party knows or reasonably believes, UI/Eversource's systems storing or hosting Confidential Information, or (F) Receiving Party receives any complaint, notice, or communication which relates directly or indirectly to (x) Receiving Party's Processing of Confidential Information or Receiving Party's compliance with Technical and Organizational Measures or applicable law in connection with Confidential Information or (y) the cybersecurity of products and services provided to UI/Eversource by Receiving Party.

e) "Losses" shall mean all losses, liabilities, damages, and claims and all related or resulting costs and expenses (including, without limitation, reasonable attorneys' fees and disbursements and costs of investigation, litigation, settlement, judgment, interest and penalties).

f) "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 upon Confidential Information, whether or not by automatic means, including, without limitation, collection, recording, organization, storage, access, adaptation, alteration, retrieval, consultation, retention, use, disclosure, dissemination, exfiltration, taking, removing, copying, making available, alignment, combination, blocking, deletion, erasure, or destruction.

g) "Technical and Organizational Measures" means security measures, consistent with the type of Confidential Information being Processed and the services being provided by Receiving Party, to protect Confidential Information, which measures shall implement industry accepted protections which may include physical, electronic and procedural safeguards to protect the Confidential Information supplied to Receiving Party against any Data Security Incident, and any security requirements, obligations, specifications or event reporting procedures set forth in this Agreement or in any Schedule to this Agreement. As part of such security measures, Receiving Party shall provide a reasonably secure environment for all Confidential Information and any hardware and software (including servers, network, and data components) to be provided or used by Receiving Party as part of its performance under the Agreement.

2. The term Confidential Information does not include any information or documents that (i) at the time of disclosure or thereafter is generally available to the public (other than as a result of a disclosure in violation of this Agreement or any other confidentiality agreement), (ii) was available to Receiving Party on a non-confidential basis from a source other than UI/Eversource, provided that such source is not bound by a confidentiality agreement, or (iii) has been independently acquired or developed by Receiving Party independent of and without reference to any Confidential Information and without violating any of its obligations under this Agreement. The exceptions described above shall not apply to Confidential Information.

3. Receiving Party agrees that UI/Eversource has the final determination in whether to provide any requested Confidential Information to Receiving Party. UI/Eversource may

refuse to provide any requested Confidential Information at its sole and absolute discretion. Receiving Party agrees that the Confidential Information it receives from UI/Eversource, or their affiliates is proprietary, the property of UI/Eversource, and shall be kept strictly confidential. The confidential information shall not be sold, traded, duplicated, published or otherwise disclosed by the Receiving Party to anyone in any manner whatsoever. Receiving Party shall use and reproduce the Confidential Information only to the extent necessary to further the Purpose. Except as expressly provided in Paragraph 4 below, Receiving Party agrees that it shall not disclose any Confidential Information of UI/Eversource to any other party without the prior written consent of UI/Eversource.

4. Receiving Party may disclose Confidential Information only to those of its employees or its consultants who need to know such Confidential Information in order to further the Purpose and who have agreed in writing to be bound by terms and conditions substantially similar to, and no less restrictive, with respect to limitations on use and disclosure, than those of this Agreement. Receiving Party shall be responsible for any breaches of confidentiality obligations committed by its employees or consultants with respect to the Confidential Information.

5. Regarding the Processing of Confidential Information, the parties agree that:

(i) Receiving Party shall Process Confidential Information only on behalf of UI/Eversource, on the instruction of UI/Eversource and in accordance with the Agreement and privacy and security laws applicable to Receiving Party's services or Receiving Party's possession or Processing of Confidential Information. UI/Eversource hereby instruct Receiving Party, and Receiving Party hereby agrees, to Process Confidential Information only as necessary to perform Receiving Party's obligations under the Agreement and as further described below and for no other purpose. For the avoidance of doubt and without limitation, (i) Receiving Party shall not Process Confidential Information for any purpose other than providing the services specified in the Agreement nor for any purpose outside the scope of the Agreement; and (ii) Receiving Party is prohibited from (w) selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, Confidential Information to any business or third party (x) retaining, using, or disclosing Confidential Information for any purpose other than for the purposes specified in the Agreement and this Agreement, (y) retaining, using or disclosing Confidential Information outside of the direct business relationship between UI/Eversource and Receiving Party pursuant to the Agreement, and (z) combining Confidential Information received from UI/Eversource with Confidential Information received from or on behalf of another person or persons or collected by Receiving Party.

(ii) The Parties agree that:

- The Processing activities that will be carried out by Receiving Party are: provide an NWS proposal to UI/Eversource using the information provided for UI/Eversource's consideration. If awarded the NWS contract, the Receiving Party shall

be responsible for fully installing and integrating the NWS Proposal selected with modifications requested, if any, by UI/Eversource.

- The categories of Confidential Information that will be Processed by Receiving Party include but not limited to: data provided through competitive solicitation process which contains granular electric system level data, project specific information, and more.

- The categories of Confidential Information subjects whose information will be processed by Receiving Party are: Business Confidential and Critical Energy Infrastructure Information.

- The instructions for the Processing of Confidential Information include but not limited to: review provided information and secure the information per UI/Eversource's guidelines established herein.

- The duration of the Processing shall be: about 6 months during the competitive solicitation phase or if awarded the NWS contract quarterly to ensure the functionality of NWS technology and shall take no more than four months or as requested.

(iii) Receiving Party shall immediately inform UI/Eversource if in Receiving Party's opinion a Processing instruction given by UI/Eversource may infringe the privacy and security laws applicable to Receiving Party's services or Receiving Party's possession or Processing of Confidential Information.

6. In the event that the activities to be carried out by Receiving Party under the Agreement do not require access to Confidential Information, Receiving Party, its employees and representatives shall be prohibited from accessing and Processing Confidential Information. If they gain access to Confidential Information, Receiving Party shall immediately inform UI/Eversource. Notwithstanding the foregoing, any Processing of Confidential Information by Receiving Party shall be subject to the terms and conditions set forth in this Agreement.

7. Receiving Party shall have in place appropriate and reasonable Technical and Organizational Measures to protect the security of Confidential Information and prevent a Data Security Incident, including, without limitation, a Data Security Incident resulting from or arising out of Receiving Party's internal use, Processing or other transmission of Confidential Information, whether between or among Receiving Party's subsidiaries and affiliates or any other person or entity acting on behalf of Receiving Party. Taking into account the state-of-the-art, the costs of implementation, and the nature, scope, context and purposes of the Processing as well as the risks of varying likelihood and severity for, among other, the rights and freedoms of the data subjects, Receiving Party shall implement Technical and Organizational Measures to ensure a level of security appropriate to the risk. Without limiting the generality of the foregoing, the Receiving Party shall implement measures to:

(A) Ensure the continued confidentiality, integrity, availability and resilience of Processing systems and services;

(B) Quickly restore availability and access to Confidential Information in the event of a physical or technical incident;

(C) Verify and evaluate, on a regular basis, the effectiveness of the Technical and Organizational Measures implemented;

(D) Pseudonymize and encrypt Confidential Information, where applicable;

(E) Safely secure or encrypt all Confidential Information, during storage or transmission; and

(F) Except as may be necessary in connection with providing services to UI/Eversource (and provided that immediately upon the need for such Confidential Information ceasing, such Confidential Information is immediately destroyed or erased), not use or maintain any Confidential Information on a laptop, hard drive, USB key, flash drive, removable memory card, smartphone, or other portable device or unit; and ensure that any such portable device or unit is encrypted.

(G) All files (e.g. – Excel, CSV, Word, etc.) shall have Microsoft Information Rights Management controls and protections applied to them.

8. To the extent that Receiving Party processes Confidential Information of Connecticut consumers as such terms are defined in An Act Concerning Personal Data Privacy and Online Monitoring (Public Act No. 22-15), the terms and conditions of Schedule C shall apply.

9. Receiving Party represents that the security measures it takes in performance of its obligations under the Agreement and this Agreement are, and shall at all times remain, at the highest of the following: (a) Privacy & IT Security Best Practices (including, but not limited to, National Institute of Standards and Technology ("NIST") SP 800-53, International Standardization Organization ("ISO") 27001/27002, Control Objectives for Information Technologies ("COBIT") framework, Center for Internet Security ("CIS") Security Benchmarks, and Top 20 Critical Controls) and (b) any security requirements, obligations, specifications, or event reporting procedures set forth in Schedule A.

10. Receiving Party shall notify UI at asoc@avangrid.com or (855)548-7276 or Eversource at CSIRT@eversource.com no later than one (1) day from the date of obtaining actual knowledge of any Data Security Incident, or from the date the Receiving Party reasonable believes that a Data Security Incident has taken place, whatever is earlier, and at Receiving Party's cost and expense, assist and cooperate with UI/Eversource concerning any disclosures to affected parties and other remedial measures as requested by UI/Eversource or required under applicable law. If the Data Security Incident involves

Confidential Information Confidential Information, the following information shall be provided as a minimum:

(A) Description of the nature of the Data Security Incident, including, where possible, the categories and approximate number of data subjects affected, and the categories and approximate number of Confidential Information records affected;

(B) Contact details of the data protection officer of the Receiving Party, where applicable, or other contact person for further information;

(C) Description of the possible consequences of the Data Security Incident or violations; and

(D) Description of the measures taken or proposed to remedy the Data Security Incident, including, where appropriate, the measures taken to mitigate possible negative effects;

(i) Receiving Party designates the following contacts for the purposes of communications related to a Data Security Incident: [__ Insert name and phone number _].

(ii) Assist and cooperate with UI/Eversource to enable them to comply with its obligations under any applicable privacy or security law, including but not limited to maintaining Confidential Information secured, responding to Data Security Incidents, and, where applicable, ensuring the rights of data subjects and carrying out Confidential Information impact assessments;

11. Receiving Party shall establish policies and procedures to provide all reasonable and prompt assistance to UI/Eversource in responding to any and all requests, complaints, or other communications received from any individual who is or may be the subject of any Confidential Information Processed by Receiving Party to the extent such request, complaint or other communication relates to Receiving Party's Processing of such Confidential Information;

12. Receiving Party shall establish policies and procedures to provide all reasonable and prompt assistance to UI/Eversource 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 Information, exfiltration of Confidential Information, disclosure of Confidential Information, or misuse of Confidential Information to the extent such request, complaint or other communication relates to Receiving Party's Processing of such Confidential Information;

13. Receiving Party shall not transfer any Confidential Information across a country border, unless directed to do so in writing by UI/Eversource, and Receiving Party agrees that UI/Eversource are solely responsible for determining that any transfer of Confidential

Information across a country border complies with the applicable laws and this Agreement;

14. At the time of the execution of this Agreement, and at any time, upon UI/Eversource's request, Receiving Party shall provide evidence that it has established and maintains Technical and Organizational Measures governing the Processing of Confidential Information appropriate to the Processing and to the nature of the Confidential Information;

15. Receiving Party shall cease Processing Confidential Information and return or securely delete of, all Confidential Information subject to the Agreement and this Agreement, including all originals and copies of such Confidential Information in any medium and any materials derived from or incorporating such Confidential Information, upon the expiration or earlier termination of the Agreement, or when there is no longer any legitimate business need (as determined by UI/Eversource) to retain such Confidential Information, or otherwise on the instruction of UI/Eversource, but in no event later than ten (10) days from the date of such expiration, earlier termination, expiration of the legitimate business need, or instruction. If the Confidential Information is destroyed, UI/Eversource require a certificate of destruction. Moreover, UI/Eversource will also require a self-attestation specifying the Confidential Information that was destroyed and if any Confidential Information was not able to be destroyed and reasons why. The self-attestation shall also include the Contractor's acknowledgment that the Agreement's protections continue beyond the termination of the Contractor's use/possession of the Confidential Information. If applicable law prevents or precludes the return or destruction of any Confidential Information, Receiving Party shall notify UI/Eversource of such reason for not returning or destroying such Confidential Information and shall not Process such Confidential Information thereafter without UI/Eversource's express prior written consent. Receiving Party's obligations under this Agreement to protect the security of Confidential Information shall survive termination of the Agreement. Receiving Party agrees to certify in writing to UI/Eversource that it has complied with the provisions established in this Agreement.

16. In the event that Receiving Party becomes legally compelled in connection with a valid judicial or other governmental or regulatory order to disclose any of the Confidential Information, Receiving Party shall give UI/Eversource prompt written notice of such requirement so that UI/Eversource may seek a protective order or other appropriate remedy and/or waive compliance with the terms hereof. Receiving Party agrees to provide only that limited portion of the Confidential Information that it is advised by written opinion of counsel is legally required and to exercise its best efforts to obtain assurance that confidential treatment shall be accorded such Confidential Information.

17. This Agreement shall be interpreted, governed, and construed under the law of the State of Connecticut, regardless of its conflicts of laws principles.

18. In addition to any other insurance required to be provided by Receiving Party hereunder, Receiving Party shall also provide the Cyber-Insurance coverage meeting the

requirements specified in Schedule B, attached hereto and made part hereof. Receiving Party shall also comply with the terms and conditions in Schedule B as they relate to any insurance required to be provided by Receiving Party pursuant to this Agreement.

19. In the event that any provision of this Agreement is determined by court to be unreasonable and/or unenforceable, such court is hereby requested to and may modify such provision in such a way as to make it reasonable and enforceable. In addition, the validity or unenforceability of any provision or provisions of this Agreement shall not affect the validity or enforceability of any other provision of this Agreement, which shall remain in full force and effect.

20. UI/Eversource and Receiving Party agree that in the event of a breach of this Agreement, UI/Eversource will experience irreparable and severe injury within a short period of time and shall be entitled to equitable relief, including injunction and specific performance, in addition to all other remedies available at law or equity.

21. Notwithstanding anything in the Agreement or this Agreement to the contrary, Receiving Party shall indemnify, defend and hold UI/Eversource, its affiliates, and their respective employees, officers, representatives and contractors, harmless from and against all Losses caused by, resulting from, or attributable to Receiving Party's breach or violation of applicable laws, regulations or any of the terms and conditions of this Agreement. Receiving Party's obligation to indemnify, defend, and hold harmless shall survive termination or expiration of the Agreement and this Agreement.

22. In the event that any provision of this Agreement is determined by court to be unreasonable and/or unenforceable, such court is hereby requested to and may modify such provision in such a way as to make it reasonable and enforceable. In addition, the validity or unenforceability of any provision or provisions of this Agreement shall not affect the validity or enforceability of any other provision of this Agreement, which shall remain in full force and effect.

23. All Confidential Information and materials furnished to Receiving Party by UI/Eversource shall remain the property of UI/Eversource. Receiving Party does not acquire any rights or licenses under any intellectual property rights of UI/Eversource under this Agreement. All Confidential Information provided hereunder is provided "as is" and without warranty of any kind. Receiving Party agrees that UI/Eversource shall not be liable for any damages whatsoever related to Receiving Party's use of the Confidential Information. Nothing contained in this Agreement shall obligate UI/Eversource to provide any Confidential Information to Receiving Party. Nothing contained in this Agreement shall be construed to require either UI/Eversource or Receiving Party to enter into any transaction and/or business relationship related to the Subject Activities (or any other transaction or business relationship), and any such transaction or relationship, if any, shall be governed solely by its applicable written agreement entered into by and between UI/Eversource and Receiving Party, if any, if, when, and as executed.

24. Receiving Party's obligations to maintain confidentiality under this Agreement shall continue indefinitely, notwithstanding the return of the Confidential Information or completion or termination of the Purpose.

25. Receiving Party acknowledges and agrees that it is aware of and shall comply with United States securities laws that prohibit Receiving Party and any other person or entity who has received material non-public information about a company from purchasing or selling securities of such company while in possession of material non-public information. Receiving Party further acknowledges that the Confidential Information will contain material non-public information regarding UI/Eversource and hereby confirms that it shall take any action necessary to prevent the use of any Confidential Information in a way which might violate any applicable law, rule, regulation, stock exchange rule or disclosure requirement of the Securities and Exchange Commission.

26. Receiving Party shall not assign or transfer its rights or obligations under this Agreement without the prior written consent of UI/Eversource. This Agreement contains the entire agreement between the parties hereto with respect to the subject matter expressed in this Agreement and this Agreement may be amended or modified only with the written agreement of all of the parties. Subject to the limitations set forth in this Agreement, this Agreement will inure to the benefit of and be binding upon the parties their successors and assigns. This Agreement may be executed in two or more counterparts each of which shall be deemed an original and all of which shall constitute one and the same instrument. Facsimile or electronic execution and delivery of this Agreement is legal, valid, and binding for all purposes.

(*Signature pages follow*)

IN WITNESS WHEREOF, **UI/Eversource and Receiving Party's Personnel** have duly executed this Agreement as of the date first above written.

UI

The United Illuminating Company

By: _____

Title: _____

EVERSOURCE

Eversource Energy Service Company

By: _____

Title: _____

RECEIVING PARTY

Contractor's Name

By: _____

Title: _____

Schedule A

General Security Requirements

A. The following definitions are relevant to this General Security Requirements Schedule:

B. “Cyber-infrastructure" means electronic information and communication systems and services, as well as the information contained therein. These systems, both those housed within facilities as well as those that are cloud-based, be they proprietary or third-party, in any manner, are comprised of hardware and software for processing (creating, accessing, modifying and destroying), storing (on magnetic, electronic or other formats) and sending (shared use and distribution) information, or any combination of said elements that include any type of electronic device such as, without limitation, standard computers (desktop/laptop) with internet connections, digital storage methods used on computers (e.g. hard drives), mobiles, smartphones, personal digital assistants, data storage media, digital and video cameras (including CCTV), GPS systems, etc.

C. "Protected Information" means Confidential Information as defined in the Agreement.

D. Capitalized terms not otherwise defined in this Schedule shall have the meaning set forth in the Agreement.

E. Receiving Party must, always, know the level of information protection that should be afforded to the Protected Information as well as the corresponding standards and applicable laws and regulations, and it shall adopt the Technical and Organizational Measures adequate thereto. Receiving Party shall, at least, maintain Technical and Organizational Measures consistent with the type of Protected Information being processed and the services being provided by Receiving Party, to secure Protected Information, which measures shall implement industry accepted protections which

include physical, electronic and procedural safeguards to protect the Protected Information supplied to Receiving Party against any Data Security Incident or other security incident, and any security requirements, obligations, specifications or event reporting procedures set forth in the Agreement, the Agreement or this Schedule. As part of such security measures, Receiving Party shall provide a secure environment for all Protected Information and any hardware and software (including servers, network, and data components) to be provided or used by Receiving Party as part of its performance under the Agreement on which Protected Information is contained.

F. When the scope of the Agreement implies the use or connection of Receiving Party's Cyber-infrastructure to that of UI/Eversource, the Receiving Party shall have reasonable Technical and Organizational Measures for its protection and for the prevention of any Data Security Incident.

G. The connection between UI/Eversource's and the Receiving Party's networks is not permitted, unless expressly agreed to in writing, in which case it must be done by establishing encrypted and authenticated virtual private networks, and the number of interconnection points between the two networks must be the minimum that is compatible with the required level of availability. The connection to the Receiving Party's network shall be removed as soon as there is no need for it.

H. Direct user connections from the Receiving Party to UI/Eversource's networks are not permitted, unless authorized in writing by UI/Eversource, and only for a limited period of time.

I. If the Agreement is fully or partially performed at the Receiving Party's premises or property, the Receiving Party must establish mechanisms and procedures for physical

access to said premises or property to prevent unauthorized persons from accessing Cyber-infrastructure or Protected Information.

J. Receiving Party shall establish mechanisms and procedures for identifying, authenticating, and controlling logical access necessary to prevent unauthorized persons from accessing its Cyber-infrastructure elements and UI/Eversource's Protected Information, and, in particular:

K. Receiving Party shall have procedures based on the principle of least privilege when granting, assigning and withdrawing authorized access and permissions to its personnel or the personnel of its subcontractors, where applicable, including privileged users or administration taking into account the need for the use, the confidentiality of the Protected Information and the resources for the performance of their tasks;

L. Receiving Party shall maintain an updated inventory of the access granted and shall withdraw access from personnel who cease working in connection with the Agreement within a period of less than twenty-four (24) hours. Credentials must always be encrypted when stored and transmitted; and

M. Receiving Party shall have policies and procedures that ensure the strength of the passwords and that they are updated regularly. Passwords shall be changed during the installation processes of new hardware or software. Receiving Party's default passwords shall be changed.

N. Receiving Party shall implement Technical and Organizational Measures necessary to ensure operational continuity under applicable service level agreements (including but not limited to contingency plans, backup and recovery procedures). In particular:

O. Receiving Party shall make backup copies of the Protected Information as frequently as is required for the services being provided by Receiving Party and according to the nature of the data, establishing the appropriate procedures and mechanisms to ensure that the data can be retrieved, that only authorized Receiving Party personnel can access it and that they are transferred and stored in such a way as to prevent access or manipulation by unauthorized persons; and

P. The same security measures shall apply to backups as to the original Protected Information.

Q. In the event that UI/Eversource has expressly authorized Receiving Party to use its own IT equipment for accessing UI/Eversource's Cyber-infrastructure, the Receiving Party shall guarantee and undertake that there are adequate security measures to protect the stationary or portable IT equipment and mobile devices used to access such Cyber-infrastructure or for storing, processing or transmitting the Protected Information, including but not limited to:

R. Automatic locking if the device is left unattended for a certain period of time. User authentication shall be required for unlocking.

S. Protection against malicious software and known vulnerabilities by including patch systems and other applicable mitigations that will mitigate such vulnerabilities.

T. Updating the operating system as often as the Receiving Party requires.

    a. The Receiving Party shall maintain an action procedure should the equipment or device be lost or stolen, ensuring, to the maximum extent possible that the event be communicated promptly, Protected Information be deleted safely in

accordance with recognized standards, and access to UI/Eversource's systems or systems containing UI/Eversource's Protected Information be suspended.

b. Before equipment is reused or replaced, the Receiving Party must protect, or if applicable remove, all the Protected Information stored on it, ensuring that unauthorized personnel or third parties cannot access or recover it.

U. The Receiving Party shall establish adequate procedures to guarantee protection against loss or unauthorized processing of files, computer media and paper documents containing Protected Information and guarantee that they are destroyed when the reasons for their creation no longer apply. Extracting data from a file and downloading it to a server or delivering it electronically is considered equivalent to computer media for the purposes of complying with these measures.

a. UI/Eversource may request information concerning any Processing of Protected Information by the Receiving Party.

V. The Receiving Party shall include security measures appropriate to the nature of the Protected Information Processed in developing, maintaining, and testing the equipment that shall be used to perform the services being provided by Receiving Party. The Receiving Party shall adopt secure code development standards and ensure that no real data is used in test environments. If necessary, UI/Eversource's express written authorization shall be required, and the same security measures required for the work environment shall be applied to these test environments.

W. When the scope of the Agreement includes the supply of equipment and/or materials, the Receiving Party shall prove that best security practices and standards have been applied

for the design, fabrication, maintenance, and, where applicable, installation of the supplied equipment and/or materials, including its components.

a. For any such equipment and/or materials with information processing capacity or network connectivity options:

X. The Receiving Party shall provide evidence or certificates that guarantee design security, firmware/software updates and malware protection.

Y. The Receiving Party shall conduct periodic analyses of vulnerabilities including but not limited to penetration testing of external assets and inform UI/Eversource about any necessary updates, especially those that affect security.

Z. All internet connected devices shall be protected with adequately complex passwords that can be changed by UI/Eversource.

AA. The configuration of devices, equipment and materials shall be adjustable exclusively according to UI/Eversource's needs, and any unnecessary functionality deactivated. Should the Receiving Party conduct any configuration, documentation to that effect shall be provided.

BB. Receiving Party should fully implement the mitigation actions available on the Cybersecurity and Infrastructure Security Agency's ("CISA's") Advanced Persistent Threats ("APTs") Targeting IT Service Provider site page to protect against malicious activity. Receiving Party should implement the following specific actions consistent with those requirements:

(i) Apply the principle of least privilege to their environment, which means UI/Eversource's data sets are separated logically, and access to client networks is not shared;

(ii) Implement robust network and host-based monitoring solutions that looks for known malicious activity and anomalous behavior on the infrastructure and systems providing client services;

(iii) Ensure that log information is aggregated and correlated to enable maximum detection capabilities, with a focus on monitoring for account misuse; and

(iv) Work with UI/Eversource to ensure hosted infrastructure is monitored and maintained, either by the service provider or the client.

Schedule B

Cyber-Insurance Requirements

A. Receiving Party shall during the term of the Agreement have and maintain the following insurance coverage:

B. Cyber Errors and Omissions Policy providing coverage, on a per occurrence basis, for acts, errors, omissions, and negligence of employees and contractors giving rise to potential liability, financial and other losses relating to data security and privacy, including cost of defense and settlement, in an amount of at least $10 million dollars, which policy shall include coverage for all costs or risks associated with:

   a. Violations of data privacy or data security laws and regulations;

   b. Cyber risks, including denial-of-service attacks, risks associated with malware and malicious code, whether designed to interrupt a network or provide access to private or confidential information;

   c. Such insurance shall cover any and all errors, omissions or negligent acts in the delivery of products and services under this Agreement. Such errors and omissions insurance shall include coverage for claims and losses with respect to network risks (such as data breaches, unauthorized access/use, ID theft, invasion of privacy, damage/loss/theft of data, degradation, downtime, etc.) and intellectual property infringement, such as copyrights, trademarks, service marks and trade dress; and

   d. Other risks specific to the work performed by Receiving Party as shall be identified by UI/Eversource.

C. Such coverage shall be furnished by an insurance company with an A.M. Best Financial Strength Rating of A- or better, and which is otherwise reasonably acceptable to UI/Eversource.

D. Receiving Party warrants that the scope of all coverage evidenced to UI/Eversource pursuant to this Agreement shall be the sole responsibility of the Receiving Party to maintain at committed to levels required by this document and Receiving Party, in any event of a loss, shall take full responsibility for the payment of any policy deductible, self-insured retention, premium or retrospective premium obligation necessary to maintain coverage, and shall include coverage for any indemnification and hold harmless agreements made by the Receiving Party pursuant to this Agreement. Receiving Party's failure to pay the applicable deductible, self-insured retention, or retrospective premium shall constitute a material breach of this Agreement, with damages equal to at least the amount of insurance lost or not provided due to such breach.

E. All insurance coverage(s) provided by Receiving Party pursuant to this Agreement shall be primary and non-contributing with respect to any other insurance or self-insurance which may be maintained by UI/Eversource.

   a. The Professional Liability Insurance retroactive coverage date shall be no later than the Effective Date. Receiving Party shall maintain an extended reporting period providing that claims first made and reported to the insurance company within two (2) years after termination of the Agreement will be deemed to have been made during the policy period.

   b. Receiving Party shall ensure that (i) the insurance policy listed above contain a waiver of subrogation against UI/Eversource and its affiliates, (ii) the Professional

Liability policy names UI/Eversource and its affiliates and assignees as additional insureds, and (iii) all policies contain a provision requiring at least thirty (30) days' prior written notice to UI/Eversource of any cancellation, modification, or non-renewal.

c. Within thirty (30) days following the Effective Date, and upon the renewal date of each policy, Receiving Party will furnish to UI/Eversource certificates of insurance and such other documentation relating to such policies as UI/Eversource may reasonably request. Should in the event that UI/Eversource reasonably determines the coverage obtained by Receiving Party to be less than that required to meet Receiving Party's obligations created by this Agreement, then Receiving Party agrees that it shall promptly acquire such coverage and notify and provide UI/Eversource, in writing, confirmation that such coverage has been acquired. All insurance must be issued by one or more insurance carriers Best rated A- or better. Receiving Party's insurance will be deemed primary with respect to all obligations assumed by Receiving Party under this Agreement.

Schedule C

Connecticut Privacy Act Clauses for Processors

A. Definitions. The following definitions and rules of interpretation apply in this Schedule:

1. "Connecticut Privacy Act" means Connecticut Act Concerning Personal Data Privacy and Online Monitoring (Public Act No. 22-15). Terms defined in the Connecticut Privacy Act, including personal data and processing, carry the same meaning in this Schedule.
2. "UI/Eversource" and "Receiving Party" have the meaning set forth in the Agreement.
3. "Agreement" means the Nondisclosure Agreement to which this Schedule is appended.
4. "Receiving Party" has the meaning set forth in the Agreement.

B. Scope of Application

1. This Schedule applies only where, and to the extent that, Receiving Party processes Confidential Information that is subject to the Connecticut Privacy Act on behalf of UI/Eversource in connection with the Agreement.
2. The instructions for the processing of the Confidential Information, the nature and purpose of the processing of the Confidential Information, the type of Confidential Information subject to the processing and the duration for the processing are set forth in section [(d)(ii)] of the Agreement.
3. The rights and obligations of UI/Eversource and Receiving Party with respect to the processing of Confidential Information are set forth in the Agreement and this Schedule.

C. Processor's Connecticut Privacy Act Obligations

1. Receiving Party shall ensure that each person processing Confidential Information is subject to a duty of confidentiality with respect to the data.
2. At UI/Eversource's direction, Receiving Party shall delete or return all Confidential Information to UI/Eversource as requested at the end of the provision of the services, unless retention of data is required by law.
3. Upon reasonable request from UI/Eversource, Receiving Party shall make available to UI/Eversource all information in its possession necessary to demonstrate the processor's compliance with the obligations in sections 1 to 11, inclusive, of the Connecticut Privacy Act.
4. Receiving Party shall, allow, and cooperate with, reasonable assessments by UI/Eversource or their designated assessors, or the Receiving Party may, at its own cost, arrange for a qualified and independent assessor to conduct an assessment of the Receiving Party's policies and technical and organizational measures in support of the obligations under sections 1 to 11, inclusive, of the Connecticut Privacy Act, using an appropriate and accepted control standard or framework and assessment procedure for such assessments, and provide a report of such assessment to UI/Eversource upon request.
5. Receiving Party shall assist UI/Eversource in fulfilling UI/Eversource's obligation to respond to consumer rights requests, by taking into account the nature of processing and the information available to Receiving Party, by appropriate technical and organizational measures, insofar as reasonably practicable.

6. Receiving Party shall assist UI/Eversource in meeting UI/Eversource's obligations in relation to the security of processing the Confidential Information and in relation to the notification of a breach of security, as defined in Conn. Gen. Stat. Section 36a-701b, of the Receiving Party's system, as set forth in Section 10 of the Agreement, in order to meet UI/Eversource's obligations, taking into account the nature of processing and the information available to Receiving Party.
7. Receiving Party shall provide necessary information to enable UI/Eversource to conduct and document data protection assessments.

D. Subcontracting

1. If UI/Eversource, after they are provided with an opportunity to object to Receiving Party's selected subcontractors, authorize Receiving Party to engage subcontractors in accordance with the terms of the Agreement, any subcontractor engaged by Receiving Party to process Confidential Information shall be engaged pursuant to a written contract that requires the subcontractor to meet the obligations of Receiving Party with respect to Confidential Information set forth in this Agreement.
2. Connecticut Privacy Act Warranties
3. Receiving Party shall comply with all applicable requirements of the Connecticut.