

Integrated Energy Data Resource (IEDR) Proposed User Agreements

Prepared by:
New York State Energy Research and Development Authority (NYSERDA)
Albany, NY

State of New York
Public Service Commission

Case 20-M-0082: In the Matter of the Strategic Use of Energy Related Data.

Integrated Energy Data Resource Agreements and Process Documentation

The New York State Energy Research and Development Authority (NYSERDA) and E Source Companies LLC (E-Source) hereby submit the following agreements and process documentation for the Commission consideration and adoption. The agreements and process documentation address data quality and integrity standards, cybersecurity, and privacy as well as other requirements that the E-Source LLC and the Integrated Energy Data Resource Platform Users must comply with.

- (1) Terms of Use Agreement (Attachment 1), the Green Button Connect (GBC) User Agreement (Attachment 2), and the Account Holder Authorization Agreement (Attachment 3), collectively, “the User Agreements”.
- (2) Data Security Agreement (DSA) and Self Attestation (SA) tailored for the implementation of IEDR (Attachment 4).
- (3) IEDR Green Button Energy Service Entities (ESEs) onboarding process (Attachment 5).

The User Agreements and DSA and SA, once adopted, will be entered into by and between E-Source, as the IEDR Platform Administrator, and authorized Energy Service Entities (ESEs) and other users of the IEDR Platform. NYSERDA shall only execute the IEDR User Agreements and DSA/SA in the capacity of an authorized ESE or a user of the IEDR platform.

Background

On February 11, 2021, the Commission issued the *Order Implementing an Integrated Energy Data Resource* (IEDR Order) directing the development of an IEDR to securely collect, integrate, and provide broad and appropriate access to large and diverse sets of valuable energy-related

information on one statewide data platform.¹ The IEDR Order designated NYSERDA as the IEDR Program Sponsor and required NYSERDA to define, initiate, oversee, and facilitate the IEDR Program on behalf of New York State and obtain a qualified Program Manager. On September 28, 2021, NYSERDA entered into a contract with Deloitte Consulting LLP, the current IEDR Program Manager, to fulfill the program management responsibilities. Further, on October 13, 2022, NYSERDA competitively selected E-Source LLC as the current IEDR Development Team to fulfill the responsibility for designing, building, and operating the IEDR platform.

In April 2021, the Commission issued an *Order Adopting a Data Access Framework and Establishing Further Process* (the DAF Order,) whereby the Commission established a uniform and comprehensive Data Access Framework to govern the means and methods for accessing and protecting all energy-related information.² Further, on October 13, 2023, the Commission issued the *Order Addressing Integrated Energy Data Resource Matters* (the October 2023 Order), whereby the Commission clarified that the IEDR Platform is a “data custodian” and stated that “[t]he IEDR is such a centralized data warehouse that will function as a data custodian for the purposes of managing the energy-related data received from various sources, including from the Joint Utilities.” The October 2023 Order further required the Joint Utilities to transfer Customer Data Sets to the IEDR Administrator³ (the IEDR Development Team) without customer consent, as such a transfer is an exchange of customer data between data custodians. The October 2023 Order, in relevant parts, stated that “[a]s a data custodian, the IEDR will be governed by the DAF, which establishes the means and methods for ESEs to access Customer Data Sets and other energy-related information from the IEDR platform, while ensuring that such information is properly protected from unauthorized disclosures.” Accordingly, and as directed in the Commission’s IEDR Order, all aspects of designing and operating the IEDR Platform must comply with the framework and requirements that the Commission established for the DAF.⁴

Agreements and Process Documentation

¹ Case 20-M-0082, Proceeding on Motion of the Commission Regarding Strategic Use of Energy Related Data, *Order Implementing an Integrated Energy Data Resource*. February 11, 2021.

² CASE 20-M-0082, In the Matter of the Strategic Use of Energy Related Data, *Order Adopting a Data Access Framework and Establishing Further Process*. April 15, 2021.

³ For all intents and purposes, IEDR Administrator is synonymous with IEDR Development Team in IEDR related literature.

⁴ “...all aspects of implementing and operating the proposed IEDR must comply with any future policies adopted under a new Data Access Framework.” IEDR Order, page 15

To meet the Commission’s goal of the strategic use of energy data, the DAF Order, in relevant parts, underscored the importance of clearly identifying and mutually accepting the expectations and responsibilities placed upon the ESEs and a data custodian. In order to comply with the Commission directives and clearly identify the expectations and responsibilities to be placed upon the ESEs and E-Source, NYSEERDA and E-Source file the attached agreements and process documentation as presented in Figure 1 and discussed in detail below.

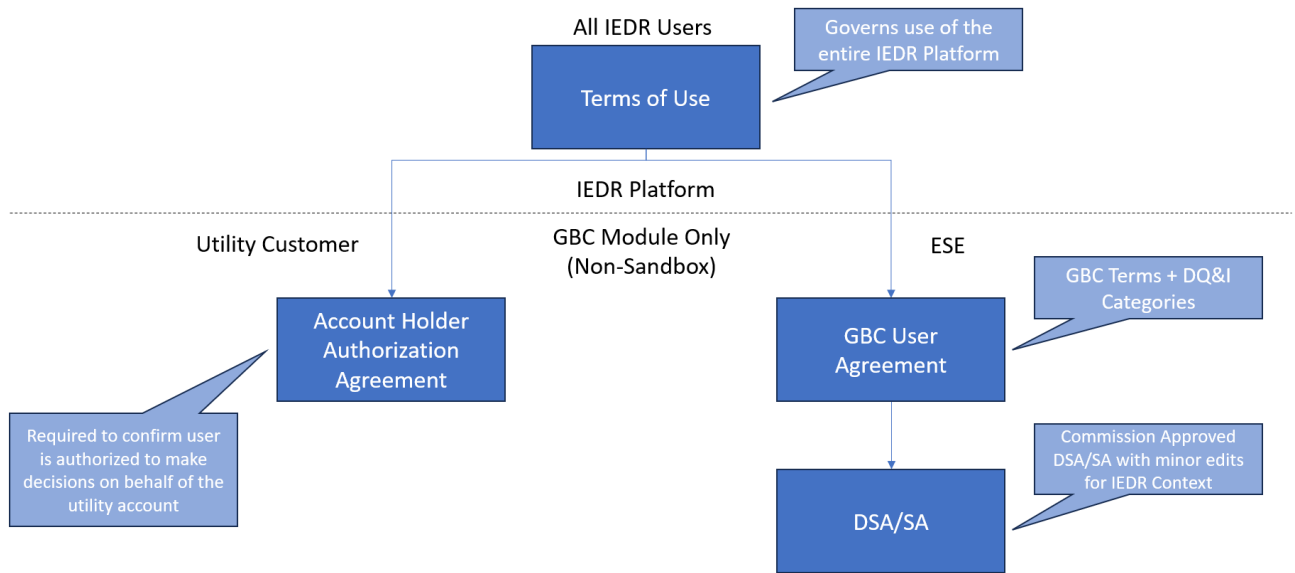


Figure 1. IEDR User Agreements: Structure and Intent

(1) User Agreements

The DAF Order required the data custodians to develop and file the User Agreement for the Commission adoption where the User Agreement is defined as “[a]n agreement between a utility or data custodian and an [Energy Service Entity or] ESE that establishes the responsibility between parties, including, among other things, the applicable data quality and integrity standards applicable to that use case or application.”⁵ The IEDR Platform is designed to enable two categories of data access – (a) publicly accessible non-confidential, yet, at times, proprietary data access for the IEDR Platform Users. Such data access will not require ESEs’ Green Button Connect onboarding or customer consent for data release; and (b) confidential, proprietary and

⁵ DAF Order, page 48.

customer consented data which will require ESE's Green Button Connect onboarding. To address the responsibilities adequately and accurately between E-Source and the IEDR Platform Users – whether for the publicly accessible non-confidential data or confidential and proprietary data, NYSERDA and E-Source propose the following three separate agreements, collectively User Agreements, for the Commission consideration and adoption. If adopted, and when entered into, together, the terms of the User Agreements delineate responsibilities between E-Source and the IEDR Platform Users including registered ESEs and utility customers.

- **IEDR Terms of Use (Attachment 1):** This agreement, as proposed, shall be entered into by and between E-Source and all IEDR users. This agreement *inter alia* establishes the general terms of use for the platform, the treatment of data, permitted use of the data, confidentiality requirements, and ownership of intellectual property. It also links to the IEDR Privacy Policy. Any updates to the IEDR Terms of Use will be posted on the IEDR Platform dashboard. This agreement would be made available on the IEDR website and as a click-through when a user registers for an IEDR account. The user would be required to acknowledge the agreement by selecting “agree” before creating and using an account on the platform.
- **Green Button Connect User Agreement (Attachment 2):** This agreement, as proposed, shall be entered into by and between E-Source and ESEs seeking to utilize the IEDR GBC module. This agreement establishes the responsibilities of both the ESE as a user and the IEDR as a data custodian, including both GBC specific terms of use for the platform and details of the data quality and integrity (DQ&I) standards defined in the DAF. In accordance with the DAF, the IEDR would “execute the GBC User Agreement in an electronic manner facilitated through a pop-up window on their GBC webpage.”⁶ An ESE would be required to select “agree”, as well as complete the rest of the IEDR GBC Onboarding Process discussed below, before having their IEDR GBC “sandbox” account

⁶ The DAF Order at p.50.

elevated to a “production” account where they could access consented utility customer data.⁷

- **Account Holder Authorization and Agreement (Attachment 3):** This agreement, as proposed, shall be entered into by and between the IEDR Administrator and a utility customer account holder seeking to share their data with a third-party via the IEDR. It sets the terms of use and consent to transfer data for a utility customer account holder specifically for the Green Button Connect application incorporated into the IEDR platform. This agreement would be made available as part of the customer consent process and a utility customer user would be required to select “agree” before data is transferred from the IEDR to the selected third party.

User Agreement Requirements:

The DAF Order created, among other things, a requirement that the applicable User Agreement “... shall include, compliance to standards associated with the data quality and integrity categories included in the Framework, as well as any other terms the data custodian and ESE must comply with.” The User Agreements submitted herein acknowledge that, in many instances, the IEDR will not be the originator of data; rather, IEDR will be a data platform facilitating streamlined and standardized access to utility data or data made available via third-party public data sources. As such, NYSERDA and E-Source request the Commission’s clarification that the Commission regulated data custodians will supply the requisite and/or agreed upon data in compliance with the Commission adopted data quality and integrity standards. NYSERDA and E-Source further request the Commission clarification that, to the extent the requisite and/or agreed upon data is obtained from data suppliers that are not subject to the Commission jurisdiction, the IEDR will not be required to the data quality and integrity standards adopted by the Commission. To the extent the data is stored and compiled within the IEDR platform, the User Agreements include an IEDR “use case specific” approach to comply with data quality and integrity categories as set forth in the DAF Order. Further, the DAF Order required the User Agreement to “be displayed in the box and by clicking the box, an ESE

⁷

will indicate they have read, understood, and agree to the terms and conditions of the agreement.” The User Agreements as proposed herein would be made available as a click-through when the users visit the IEDR and a user would be required to select “agree” to accept the terms of the User Agreements.

(2) Data Security Agreement

The DAF Order specifically requires the User Agreement to “not include the cybersecurity and privacy requirements necessary for [Green Button Connect or] GBC as those will be handled through the ESE Data Ready Certification process and reflected in a Data Access Agreement.”

The DAF Order further adopts and requires the Data Ready Certification process to “replace the current Data Security Agreement (DSA) and Self Attestation (SA) process that requires an ESE to certify it has the necessary cybersecurity and privacy requirements with each utility from which it seeks access to data.” The October 2023 Order stated that “ESE seeking access to data via the IEDR platform must comply with the policies and requirements established as part of the DAF for release of such data, including the signing of a Data Security Agreement or Data Access Agreement between the data custodian and the ESE, which details the responsibilities of both parties in protection of said data.”

NYSERDA and E-Source hereby present the IEDR DSA and SA that meets the minimum cybersecurity and privacy protections as set forth in the *Commission Order Establishing Minimum Cybersecurity and Privacy Protections and Making Other Findings*, issued October 17, 2019. While the NYSERDA and E-Source proposed DSA/SA is modeled on the existing, Commission approved DSA/SA, the agreement includes narrowly tailored edits to 1) provide ESEs appropriate IEDR specific context before entering the agreement and 2) account for the fact that the IEDR is not being operated by a regulated utility.

NYSERDA and E-Source believe these modifications are required because in the IEDR use case, the DSA will be executed between E-Source (as the IEDR Platform Administrator), not the Investor Owned Utilities, and ESEs. Examples of the proposed modifications in the IEDR DSA/SA include:

- References to the IEDR Orders in the agreement recitals to establish the regulatory context for the IEDR's DAF compliant requirements, which include an ESE's completion of the DSA/SA.
- Removing reference to "a direct connection with the Utility IT systems", because in the case of an ESE utilizing the IEDR, no such connection would ever be established by an ESE and renders such reference inaccurate.
- Establishing rights and obligations with E-Source rights and obligations (e.g., under the Provision of Information, E-Source, not a utility, is agreeing to provide to an ESE or its Third-Party Representative certain Confidential Customer Information under the proposed agreement, at the direction of a Customer).

In summary, the primary form and substance of the substantive and material data sharing and security terms and obligations are preserved; however, the draft IEDR DSA/SA proposes modifications to the parties' obligations to fit the IEDR / ESE use case as opposed to the Utility/ESE use case.

In addition, because IEDR is a digital platform granting access to utility customer and system data in a manner that's developed and approved by the Commission, for the efficiency of implementing the IEDR, and within the spirit of embarking on a statewide digital platform, NYSERDA and E Source hereby request the Commission to allow the IEDR DSA/SA be executed using an electronic manner using an electronic manner facilitated through online forms and digital acknowledgement, similar to the User Agreements. More specifically, NYSERDA and E Source request the ability to make the DSA/SA available via a "scrollwrap" agreement. The scrollwrap agreement would require an ESE to scroll through the entire agreement before they could select "agree" to accept the terms of the DSA/SA, creating a binding agreement. The IEDR will make the DSA/SA agreement available via download after the ESE selects "agree" for reference. This proposed approach would enable a streamlined process for users and will be similar to the click-through format required for the Green Button Connect User Agreement, and

there is significant precedent that “clickwrap” and “scrollwrap” agreements are legally enforceable.⁸

Green Button Connect (GBC) Onboarding Process:

The DAF Order required the Joint Utilities as data custodians to file details regarding the Green Button Connect third party onboarding process, including associated timelines specific to each utility’s onboarding procedures. In light of the Commission clarification within the October 2023 Order that the IEDR Platform is a “data custodian” and that “[t]he IEDR is such a centralized data warehouse that will function as a data custodian and will be governed by the DAF,” NYSERDA and E-Source submit the GBC Onboarding Process for Commission consideration and approval. As discussed in detail in Attachment 3, the GBC Onboarding Process includes the following steps: (i) creation of a IEDR account; (ii) confirmation that an ESE is registered with the Department of Public Service; (iii) entering of the DSA/SA; and (iv) getting approved for an access to the production environment.

Conclusion:

For the reasons discussed above, NYSERDA and E-Source sincerely request:

- (i) The Commission consideration and adoption of the User Agreements, IEDR specific DSA/SA, and GBC Onboarding Process, that will allow E-Source to enter an agreement with authorized Energy Service Entities (ESEs) and other users of the IEDR Platform in administration of the IEDR Platform.
- (ii) The Commission clarification that – (a) the Commission regulated data custodians will supply the requisite and/or agreed upon data in compliance with the Commission

⁸ New York Courts have upheld enforceability of clickwrap agreements provided that a consumer is given sufficient opportunity to read the agreement and accept it with an unambiguous method of accepting or declining the agreement. See *People ex rel. Spitzer v. Direct Revenue, LLC*, 19 Misc. 3d 1124(A), 2008 N.Y. Slip Op. 50845(U) and *Fteja v. Facebook, Inc.*, 841 F. Supp. 2d 829, 837 (S.D.N.Y. 2012). Further, the scrollwrap agreement, as proposed here, is consistent with the Commission precedent of adopting the clickthrough agreement for the Green Button Connect implementation.

adopted data quality and integrity standards, and (b) to the extent the requisite and/or agreed upon data is obtained from data suppliers that are not subject to the Commission jurisdiction, the IEDR will not be required to meet the data quality and integrity standards adopted by the Commission.

- (iii) The Commission authorization for the IEDR DSA/SA to be executed using an electronic manner facilitated through the IEDR Platform, specifically through the use of a “scrollwrap” agreement that will be binding on the parties.

Attachment 1- Terms of Use for IEDR Platform

These Terms of Use for IEDR Platform (“TOU”) govern your access to and use of the Platform (defined below) offered by E Source Companies LLC (“E Source”) and its Licensors (defined below). By using the Platform, you acknowledge and agree you have read, understand, and agree to be legally bound to these TOU. If you use the Platform on behalf of an organization, you agree to these TOU on behalf of that organization and you represent to E Source you have the authority to do so. In such case, “you” and “your” will refer to that organization. E Source and you are sometimes individually referred to as a “Party” and collectively referred to as the “Parties.” Accordingly, the Parties agree as follows:

1. The Platform.

a. E Source operates, in conjunction with its licensors and subcontractors (its “Licensors”), the Integrated Energy Data Resource online platform (the “Platform”) that allows access to public information, utility information, Utility Customer information, and other information that may or may not be confidential, personal, or proprietary, and which generally originates in the state of New York (“Data”). For purposes of these TOU, “Utility Customer” means a residential or business entity consuming services and receiving an invoice from a utility operating in the state of New York. Subject to these TOU, E Source hereby grants you a non-exclusive, revocable, and nontransferable (except in accordance with Section 12) license to access and use the Platform during the Term.

b. In order to use certain features of the Platform, you will be required to establish an account with UtilityAPI, Inc. (“UtilityAPI”), a Licensor to E Source, through which you will be able to submit requests to Utility Customers for Data and receive that Data once authorized for release. Such UtilityAPI account, to the extent used in connection with your use of or access to the Platform or Data, constitutes part of the “Platform” and such use is subject to these TOU. You acknowledge and agree that UtilityAPI, with its successors and assigns, is an intended third-party beneficiary of your representations, warranties, covenants, and agreements set forth in these TOU, with the right to enforce such provisions.

c. Use of the Platform is subject to your compliance with these TOU and all policies that further govern your access to or use of the Platform (“Policies”), including those available at [Privacy Policy](#) and [Disclaimer](#). E Source may publish or amend the Policies at any time for any reason. If you use the Platform, you will be bound by the Platform’s then-current Policies. E Source will post all updates to these TOU and the Policies and your continued use of the Platform after the modifications will constitute your: (i) acknowledgment of the modified TOU and Policies; and (ii) agreement to abide and be bound by the new TOU and Policies. E Source may change any aspect of the Platform without notice to you.

2. Use of the Platform.

a. You shall maintain the security of your log-in credentials to the Platform. You are responsible for any expense, loss, or liability caused by the loss or breach of those credentials.

b. You shall not use the Platform or any of its code or APIs to: (i) violate the security of, or gain unauthorized access to, the Platform or any computer, device or system; (ii) discover passwords or encryption codes; (iii) use any robot, spider, or retrieval application, or other device, to retrieve or index any portion of the Platform; (iv) attempt to duplicate any part of the Platform or its code, or to attempt to reverse engineer, decompile or otherwise gain access to any software component or code, or to attempt to create a substitute or competing Platform; (v) disrupt the functionality of the Platform or disrupt another user's use of or access to the Platform; (vi) access or use the Platform or the Data in a way that circumvents a contractual usage limit; (vii) circumvent any technological measures implemented to prevent framing or mirroring of any part of the Platform; (viii) store or transmit (A) malicious code, viruses, or spam, (B) unsolicited marketing communications, (C) infringing, libelous, or otherwise unlawful or tortious material, or (D) any material in violation of third-party proprietary, privacy, or similar rights; or (ix) promulgate any unfair or deceptive practices or in contravention of any law or administrative rules or regulations (including but not limited to the federal CAN-SPAM regulations and the TCPA).

c. You agree to be responsible for your authorized users' compliance with these TOU, use commercially reasonable efforts to prevent unauthorized access to or use of Platform, and notify E Source promptly of any such unauthorized access or use.

d. You represent and warrant that you will comply with all applicable laws, regulations, and duties applicable to your use of the Platform and your collection, use, and treatment of Data. You understand that none of E Source or its Licensors has any obligation to, and will not, advise you as to such laws, regulations, and duties.

e. When you send e-mail to us, you are communicating electronically and you consent to receive communications from us electronically. You agree that all agreements, notices, disclosures, and other communications that we provide to you electronically, via the Platform or otherwise, satisfy any legal or contractual requirement that such communications be in writing.

3. Data, Usage Data, and Anonymized Data.

a. The Data made available through the Platform is obtained from various sources and is provided for informational purposes only. None of E Source, its Licensors, and responsible parties make any representations or assurances as to the accuracy, completeness, reliability, or suitability of the Data. The Data may be subject to errors, omissions, changes, or updates without notice. E Source, its Licensors, and responsible parties are not liable for any damages or losses arising from your use of or reliance on the Data.

b. Subject to these TOU, E Source hereby grants you a non-exclusive, revocable, nonsublicenseable, nontransferable license to access and use the Data that is made available to you through the Platform during the Term for your personal or internal business use.

c. You grant E Source (including any Licensors, hosting providers, or other contractors acting on its behalf) a worldwide, non-exclusive, perpetual, irrevocable, royalty-free license to access, use, copy, distribute, perform, and display data and information submitted by you through the Platform, including account information, and information collected from your use of the Platform, such as request logs and session cookies ("Usage Data"): (i) as reasonably necessary to

provide the Platform; (ii) to prevent or address service or technical problems or in connection with customer support matters; (iii) to improve or modify the Platform; and (iv) as compelled by law or as otherwise permitted in writing by you.

E Source and its Licensors may aggregate, anonymize, or otherwise de-identify any information or data, including Usage Data, collected from you or your authorized users and use and disclose such information or data without restriction, provided such aggregated, anonymous, or otherwise de-identified information or data does not individually identify you (“Anonymized Data”) prior to disclosure to a third party, except that E Source or such Licensor may disclose individually identifiable information or data to its licensors or contractors who are subject to confidentiality obligations. E Source or such Licensor, as applicable, retains all intellectual property rights in Anonymized Data.

4. Confidentiality.

a. As a condition of the licenses granted in Sections 1 and 3, you agree to treat all Data and other information disclosed through the Platform as confidential, unless and until such information has been made generally available to the public through no fault of yours.

b. You shall not reproduce or distribute the Data or other information available through the Platform, in whole or part, other than as required by law or a court order, in any judicial, administrative or governmental proceeding, subject to your prior notification to E Source, to the extent such notice is legally permitted.

c. On termination of these TOU, you shall promptly destroy all copies, whether in written, electronic, or other form, of the Data and other information provided by the Platform.

5. Intellectual Property.

a. As between the Parties, E Source and/or its Licensors own all right, title, and interest, including all intellectual property rights, in and to the Platform, and the Platform remains the sole property of E Source and/or its Licensors. No rights to the Platform are granted to you hereunder other than as expressly set forth herein.

b. E Source and/or its Licensors own all right, title, and interest in all intellectual property rights in its and their domestic and foreign trademarks, service marks, trade names, logos, and domain names (“Marks”), and all Anonymized Data collected or stored in connection with the Platform.

c. E Source and/or its Licensors may use any feedback received from you to create, develop, or modify the Platform or any other concept, brand, software code, product, or feature (“Improvements”), and E Source or the applicable Licensor owns all intellectual property rights in such Improvements. If you are deemed to have any ownership interest or rights in an Improvement, then you hereby assign all of those interests and rights to E Source or the applicable Licensor.

6. Term and Termination. The term of these TOU commences on the day you begin using the Platform and continues until these TOU are terminated (“**Term**”). Either Party may terminate

these TOU for any reason by giving the other Party written notice and, upon such termination, your right to use the Platform will immediately terminate. E Source may, with or without notice, suspend, terminate, or otherwise deny your or any other person's access to or use of all or any part of the Platform (and UtilityAPI may terminate your access to your UtilityAPI account), without incurring any resulting obligation or liability. Sections 2.d., 3.c., and 4-12 shall survive the expiration or termination of these TOU and any termination of your use of the Platform.

7. Due Authority. Each Party represents that it has validly entered into these TOU and has the legal power to perform all of its obligations hereunder.

8. Disclaimer of Warranties. Except as set forth in Section 7, E Source and its Licensors hereby disclaim all warranties, representations, or guarantees of any kind related to the Platform or Data. YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT YOUR USE OF THE PLATFORM AND DATA IS AT YOUR SOLE RISK AND THE PLATFORM AND THE DATA ARE PROVIDED "AS IS" AND WITHOUT REPRESENTATION OR WARRANTY OF ANY KIND FROM E SOURCE AND/OR ITS LICENSORS, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, LACK OF VIRUSES, COMPATIBILITY WITH THE PLATFORM, OR NON-INFRINGEMENT OF THIRD-PARTY RIGHTS.

9. Limitation of Liability. NEITHER E SOURCE NOR UTILITYAPI NOR ANY OF E SOURCE'S OTHER LICENSORS WILL BE LIABLE (WHETHER IN CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE, PRODUCT LIABILITY, OR OTHER THEORY), OR OTHERWISE) TO YOU OR ANY OTHER PERSON FOR COST OF COVER, RECOVERY, OR RECOUPMENT OF ANY INVESTMENT MADE BY YOU OR YOUR AFFILIATES IN CONNECTION WITH THESE TOU OR THE PLATFORM, OR FOR ANY LOSS OF PROFIT, REVENUE, BUSINESS, OR DATA OR PUNITIVE, SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR RELATING TO THESE TOU OR THE PLATFORM, EVEN IF ADVISED OF THE POSSIBILITY OF THOSE COSTS OR DAMAGES. FURTHER, E SOURCE'S AND ITS LICENSORS' COLLECTIVE AGGREGATE LIABILITY ARISING OUT OF OR IN CONNECTION WITH THESE TOU AND/OR YOUR USE OF THE PLATFORM OR ANY DATA WILL NOT EXCEED AT ANY TIME \$100. THE DISCLAIMERS AND EXCLUSIONS AND LIMITATIONS OF LIABILITY CONTAINED IN SECTION 8 AND THIS SECTION 9 ARE A MATERIAL PART OF E SOURCE'S AGREEMENT TO PROVIDE THE PLATFORM TO YOU AND SHALL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY, AND SHALL APPLY TO THE FULLEST EXTENT PERMITTED BY LAW.

10. Indemnification. You will defend, indemnify, and hold harmless E Source and UtilityAPI, and its and their officers, directors, employees, agents, and contractors, against any third-party claim, loss, damage, settlement, cost, expense, or other liability (including, without limitation, attorneys' fees) (each, a "Claim") arising from or related to (i) your actual or alleged breach or violation of these TOU, and (ii) any breach of Data or security breach of the Platform associated with your log-in credentials or any other acts or omissions by you. You may not consent to the entry of any judgment or enter into any settlement of a Claim without the prior written consent of E Source or UtilityAPI, as applicable, which may not be unreasonably withheld.

11. Governing Law and Venue. These TOU and any dispute, proceeding, or claim of any nature arising out of or in any way relating to these TOU shall be governed by the laws of the State of New York, without regard to its choice of law rules, and the Parties hereby irrevocably and unconditionally submit to the exclusive jurisdiction of the state and/or federal courts sitting in New York, New York, in all matters arising out of or in any way relating to these TOU.

12. Miscellaneous. These TOU shall not be transferred or assigned by you without the written consent of E Source. E Source may transfer its rights and obligations under these TOU in conjunction (i) with a sale of all or substantially all of its assets or equity, (ii) with a merger or similar transaction, or (iii) to another entity that takes over the Platform; provided the acquiring or resulting entity agrees to be bound by these TOU. Any purported assignment in violation of this Section is void. No waiver of any term or condition in these TOU shall be deemed a further or continuing waiver of such term or condition or a waiver of any other term or condition, and any failure of a party to assert a right under these TOU shall not constitute a waiver of such right or provision. If any provision of these TOU is found to be illegal or unenforceable, the other provisions shall remain effective and enforceable to the greatest extent permitted by law. Failure to enforce these TOU shall not constitute a waiver of any term hereof. All notices must be in writing and sent to the other Party through the contact information provided in the Platform. Notices are deemed effective upon receipt. Nothing herein shall be construed as creating a partnership, joint venture, or agency or any other relationship. Except for any Data Sharing and Services Agreement that may have been separately entered into by the Parties, these TOU are the entire understanding between the Parties regarding its subject matter and supersede all prior understandings and agreements, whether oral or written, regarding that subject matter. Other than UtilityAPI and the indemnitees set forth in Section 10, there are no third-party beneficiaries to these TOU.

13. Support. User support is available by contacting iedr-support@esource.com. Certain services may offer separate or additional user support. Support may not be available for preview or beta versions of certain features.

Attachment 2- The Integrated Energy Data Resource Green Button Connect User Agreement

NOTICE: YOU ACKNOWLEDGE THAT YOU HAVE READ AND AGREE TO COMPLY WITH THE FOLLOWING TERMS AND CONDITIONS THAT GOVERN YOUR USE OF THE IEDR GREEN BUTTON CONNECT (GBC) PLATFORM. IF YOU DO NOT AGREE TO COMPLY WITH THE IEDR GBC TERMS AND CONDITIONS, DO NOT PROCEED WITH THE GREEN BUTTON CONNECT REGISTRATION PROCESS.

If you use the Platform on behalf of an organization, you agree to this Agreement on behalf of that organization and you represent and warrant to E Source that you have the authority to do so. In such case, “you” and “your” will refer to that organization. E Source and you are sometimes individually referred to as a “Party” and collectively referred to as the “Parties.”

1. Introduction

E Source operates the Integrated Energy Data Resource online platform (the “Platform”) that allows parties to access certain public information, utility information, utility Customer information, and other information that may or may not be confidential, personal, or proprietary, and which generally originates in the state of New York.

By agreeing to these terms and conditions (“IEDR GBC Terms”), you acknowledge that you are aware of and agree to comply with the terms of all applicable state and federal laws and rules, and other consumer privacy rules and cybersecurity requirements referenced in the Data Security Agreement (DSA) and Self-Attestation (Exhibit A of the DSA), as well as to comply with privacy rules, laws, and regulations referenced in the [IEDR Privacy Policy](#) and [TOU](#), which laws and rules are incorporated and made a part of these IEDR GBC Terms by reference and as the laws, rules orders and utility practices may change from time to time. Upon your completion of the Green Button Connect (GBC) Business Onboarding Process or Data Ready Certification to access GBC data through the IEDR, IEDR and your executed agreement to comply with the terms and conditions specified herein, the IEDR GBC Terms shall constitute the “GBC User Agreement” (this “Agreement”) between you and IEDR.

The terms of this Agreement shall remain in force and apply for the duration of your use of the IEDR Platform. No utility data may be used to provide non-utility products or service to Customers without the Customer’s consent.

2. Definitions

The following terms shall have these defined meanings for purposes of this Agreement:

“Applicant” means the Energy Services Entity (ESE) registering to use the IEDR Platform.

“Authorization End Date” means, as selected by Customer, the date when on-going (future) data access is discontinued.

“Commission” means the New York Public Service Commission (PSC).

“Customer” means a customer of a New York State utility company, the New York Power Authority, or the Long Island Power Authority.

“Customer Data” means collectively, any and all data and information of or concerning any identified or identifiable Customer through GBC.

“Data” means public information, utility information, Customer Data, and other information that may or may not be confidential, personal, or proprietary, and which generally originates in the state of New York.

“Data Security Agreement” or “DSA” means the terms and conditions of the Data Sharing and Services Agreement between ESE and E Source, including cybersecurity and privacy requirements, applicable to Applicant or ESE when seeking access to energy-related data.

"E-Source Data" means data held by E-Source, whether produced in the normal course of business or at the request of ESE.

“Energy Services Entity” or “ESE” means an entity that provides energy or performs an energy-related service.

“Green Button Connect” or “GBC” provides a set of standards for allowing interoperable communications of energy usage and billing information between utilities and Applicant or ESE.

“Incident” means an actual or suspected breach or compromise of the privacy, security, confidentiality or integrity of (i) confidential and/or protected information (including, without limitation, Customer Data), (ii) the IEDR Platform, or (iii) any other IEDR information systems.

“UBP” means the Uniform Business Practices for DER as adopted and modified by the Commission.

3. Term and Termination

The term of this Agreement commences on the earlier of (i) the day that you begin using the Platform, or (ii) the day that you click “Agree”, and continues for the same duration as the DSA.

4. Discontinuance and Modification

E Source reserves the right to change any aspect of the Platform without notice to you.

E Source will use commercially reasonable efforts to provide that (i) the Platform is updated and functional, and (ii) all Data transmitted through the Platform is provided to You in a reliable, standardized, and usable format. Notwithstanding the foregoing, you acknowledge and agree that the Platform may experience downtime for routine or emergency maintenance and certain technical issues could arise with the availability and/or accuracy of the Data. In the event that the Platform is expected to experience downtime for routine maintenance, E Source shall notify You through a banner or other notification available on the Platform.

E Source will not be liable if for any reason if all or any part of the IEDR GBC Platform is unavailable at any time or for any period. If E Source is made aware of an error with the Platform, E Source shall make a commercially reasonable effort to resolve the issue as further described within this Agreement.

5. Data Quality & Integrity Standards

Unless otherwise specified, you acknowledge and agree that the Data is sourced from certain public and non-public sources, and is not originated by E-Source or the Platform. You acknowledge and agree that E Source has no obligation to verify the accuracy, completeness, or reliability of the Data that is transmitted to the Platform, E Source is not responsible for the specific content of the Data as provided by third party sources, and E Source makes no representations or warranties that the Data from third-party sources is accurate, reliable, or complete. E Source shall use commercially reasonable efforts to maintain the integrity of the Data as it was received by E Source from third parties.

You are not entitled to, and you agree not to seek, any monetary remedies, including any damages, for E-Source's failure to comply with the Data Quality and Integrity Standards listed below:

1. Adherence to a standardized data format specific to the data access mechanism;

The IEDR GBC Platform leverages the data format standards for Green Button Connect My Data, located at: https://www.naesb.org//ESPI_Standards.asp

2. Maximum percentage of data that includes redundant or extraneous entries;

As the Data is sourced from public and non-public third-party sources, unless otherwise specified, the maximum percentage of Data that includes redundant or extraneous entries and the maximum percentage of data errors will be determined by each data custodian supplying Data to the Platform. To the extent that E Source recognizes or is informed of redundant or extraneous entries, E Source will take steps to remove the redundant or extraneous entries.

After investigations performed by E Source, in instances where the IEDR is the source of the redundant or extraneous entry, E Source will document the frequency in comparison to redundant or extraneous entries provided by 3rd parties.

3. Maximum percentage of data errors;

E Source does not verify the accuracy, completeness, or reliability of the Data that is transmitted through the Platform, and E Source is not responsible for the specific content of the Data. The Data is sourced from certain public and non-public sources, and is not originated by E Source or the Platform. E Source makes no representations or warranties that the Data is accurate, reliable, or complete. To the extent that E Source recognizes or is informed of data errors, E Source will take steps to resolve the Data errors.

After investigations performed by E Source, in instances where the IEDR is the source of the data error, E Source will document the frequency in comparison to redundant or extraneous entries provided by 3rd parties.

4. Maximum amount of time it will take to transfer data;

The speed at which the data is transferred from the IEDR to an end-user is dependent upon the size of the data and the speed with which the end-user can access and download it. E Source is not responsible for any third-party download speeds, and therefore cannot accurately quantify a maximum amount of time that it will take to transfer the data to an end-user. However, E Source anticipates most data transfer will be available within 24 hours.

5. Maximum amount of time to acknowledge a reported data error;

If E Source is made aware of an error with the Data, then such incident shall be logged into E Source's system with a case assignment to a technician and notification (via phone call, email or pager) within one business day of a case being opened.

6. Maximum amount of time to resolve a data error;

E Source's goal is to resolve reported errors in Data within ten (10) business days of receipt of adequate cooperation from the applicable electric, gas, or steam utility operating in the state of New York.

7. Notification of data access mechanism outage or downtime;

Scheduled Maintenance – E Source will use commercially reasonable efforts to provide at least 24 hours advanced notice by publication for non-downtime service actions. E Source's normal maintenance window will be between 10:00 PM and 5:00 AM Eastern Time.

Scheduled Downtime – E Source will use commercially reasonable efforts to provide at least 72 hours for maintenance that will be service interrupting. Notice will be provided by publication. Scheduled downtime is intended to be limited to the time between 10:00 PM Saturday and 5:00 AM Sunday Eastern Time.

8. Conformance to application standard, including third-party certification, if one exists, such as for GBC

The IEDR GBC Platform has been certified compliant with the GBC standard by the Green Button Alliance.

9. Technical support information, such as contact and maximum amount of time to respond to and resolve issues that arise.

E Source shall take prompt action upon recognition of a failure of the Platform or of an error in the Data. If you believe that you are experiencing a service disruption, you should email iedr-support@esource.com.

E Source shall maintain a dashboard to inform you of current and historical outages. E Source will update this dashboard after discovery of a service disruption, usually within 30 minutes thereafter.

6. DSA Incorporation

The Data Security Agreement (DSA), together with any necessary conforming changes, are incorporated and made a part of this Agreement by reference.

Attachment 3- Account Holder Authorization Agreement⁹

This Account Holder Authorization and Agreement (this “Agreement”) sets forth terms and conditions pursuant to which E Source Companies LLC (“E Source”) provides an integrated energy data resource online platform (“IEDR Platform”). The IEDR Platform facilitates a service as set forth below that allows you to share data regarding your customer account, contact information, utility billing, and energy usage data (“Customer Data”) through your account with your utility provider (“Utility”) with certain third parties authorized by You (“Authorized Parties”) (the “Service”).

Prior to your use of the Service or the IEDR Platform, you must indicate your acceptance of this Agreement. By clicking “Agree”, you indicate that you have read, understand, and agree to this Agreement. If you use the Service or the IEDR Platform on behalf of an organization, you agree to this Agreement on behalf of that organization and you represent and warrant to E Source that you have the authority to do so. In such case, “you” and “your” will refer to that organization. E Source and you are sometimes individually referred to as a “Party” and collectively referred to as the “Parties.” Accordingly, the Parties agree as follows:

1. **Use of the Service or the IEDR Platform.** By accepting this Agreement:
 - a. you acknowledge and agree to the terms and conditions of this Agreement, the Terms of Use available at [URL], and the Privacy Policy available at [URL];
 - b. you represent and warrant to E Source that you are the customer of record of the applicable utility account and are fully authorized to give instructions and consents in connection with the account and the Customer Data;
 - c. you acknowledge and agree that the purpose of the Service is to transmit your Customer Data to Authorized Parties, and you hereby authorize E Source to make such disclosure through the IEDR Platform. The Service is optional and you may revoke the authorization at any time by using the “Revoke” function within the Service. You recognize, however, that once your Customer Data has been shared with an Authorized Party, E Source will have no control over, and will not monitor, such Authorized Party’s management or use of your Customer Data. Similarly, revocation of such authorization will not result in any Authorized Parties returning or destroying your Customer Data. If you decide to share your Customer Data with any third parties, you do so entirely at your own risk; and
 - d. **BY AGREEING TO ALLOW E SOURCE TO DISCLOSE CUSTOMER DATA TO AN AUTHORIZED PARTY, (I) YOU HEREBY RELEASE, DISCHARGE, AND WAIVE ALL RIGHTS THAT YOU HAVE OR THAT MAY ACCRUE IN THE FUTURE AGAINST E SOURCE, ITS**

⁹ This Agreement was adopted by the New York State Public Service Commission Order (reference/citation TBD)

SUBCONTRACTORS, AND YOUR UTILITY COMPANY RELATING TO YOUR AGREEMENT TO ALLOW THE DISCLOSURE OF CUSTOMER DATA TO AN AUTHORIZED PARTY (INCLUDING AN AUTHORIZED PARTY'S USE, MISUSE, OR UNAUTHORIZED DISCLOSURE OF SUCH CUSTOMER DATA), INCLUDING BASED ON BREACH OF CONTRACT, BREACH OF EXPRESS AND/OR IMPLIED WARRANTY, MISREPRESENTATION, NEGLIGENCE, NEGLIGENT MISREPRESENTATION, AND GROSS NEGLIGENCE, (II) YOU AGREE TO FOREVER REFRAIN FROM INSTITUTING, INITIATING, PROSECUTING, MAINTAINING, OR VOLUNTARILY PARTICIPATING IN ANY LAWSUIT, CLAIM, LITIGATION, DEMAND, CAUSE OF ACTION, OR OTHER PROCEEDING IN ANY JURISDICTION OR FORUM AGAINST E SOURCE, ITS SUBCONTRACTORS, OR YOUR UTILITY COMPANY RELATED TO SUCH DISCLOSURE OR THE AUTHORIZED PARTY'S USE, MISUSE OR UNAUTHORIZED DISCLOSURE OF SUCH CUSTOMER DATA, AND (III) YOU WILL LOOK ONLY TO AN AUTHORIZED PARTY FOR RECOURSE REGARDING THAT AUTHORIZED PARTY'S USE, MISUSE, OR UNAUTHORIZED DISCLOSURE OF CUSTOMER DATA. THE RELEASES, WAIVERS, AND COVENANTS NOT TO SUE IN THIS PARAGRAPH SHALL APPLY TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW.

2. License to Customer Data. You grant E Source and its licensors a worldwide, non-exclusive, perpetual, non-expiring and transferable license to access, use, copy, and provide to Authorized Parties the Customer Data for any reason related to the Service or the IEDR Platform.

3. Term and Termination. The term of this Agreement commences when you click "Agree", and continues as long as you are using the IEDR Platform, unless and until terminated as set forth below or you permanently cease use of the IEDR Platform. E Source may terminate this Agreement at any time and for any reason. Termination of this Agreement shall not result in the automatic revocation of the license granted in Section 2. In the event of termination of this Agreement, you are required to follow the process set forth in Section 1.c to revoke any authorization granted prior to termination. You acknowledge and agree that E Source and any Authorized Parties will continue to have the right to use the Customer Data as set forth herein.

4. Indemnification. You will defend, indemnify, and hold harmless E Source, Authorized Parties, and its and their subsidiaries, affiliates, officers, directors, employees, agents, and licensors, against any third-party claim, loss, damage, settlement, cost, expense, or other liability (including attorneys' fees) arising from or related to (i) your non-compliance with applicable laws, (ii) your actual or alleged breach or violation of this Agreement, (iii) your use of the Services and the IEDR Platform, and (iv) E Source's or the Authorized Party's use of or reliance on the Customer Data as permitted under this Agreement.

5. Limitation of Liability. YOU AGREE THAT NEITHER E SOURCE OR THE UTILITY, NOR ANY OF ITS OR THEIR SUBSIDIARIES, AFFILIATES, AGENTS, LICENSORS, OR SERVICE PROVIDERS SHALL BE LIABLE FOR ANY DAMAGES WHATSOEVER, WHETHER DIRECT, INDIRECT, CONSEQUENTIAL, SPECIAL, OR PUNITIVE, OR FOR LOSS OF PROFITS OR OTHER ECONOMIC LOSS, AND REGARDLESS OF WHETHER THE CLAIM ARISES IN CONTRACT, TORT (INCLUDING NEGLIGENCE), EQUITY, OR UNDER ANY OTHER THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH (i) THIS

AGREEMENT, (ii) YOUR USE OF THE SERVICE OR THE IEDR PLATFORM, (iii) ANY USE OR RELIANCE UPON CUSTOMER DATA OR OTHER INFORMATION CONTAINED IN OR ACCESSED FROM THE SERVICE OR THE IEDR PLATFORM, OR (IV) THE DISCLOSURE OF CUSTOMER DATA TO AUTHORIZED PARTIES, WHETHER OR NOT E SOURCE, THE UTILITY, OR ANY OF ITS OR THEIR SUBSIDIARIES, AFFILIATES, AGENTS, LICENSORS, OR SERVICE PROVIDERS HAVE BEEN ADVISED OF THE POSSIBILITY OF THOSE DAMAGES OR SUCH DAMAGES WERE REASONABLY FORESEEABLE. FURTHER, E SOURCE'S AGGREGATE LIABILITY ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT WILL NOT EXCEED AT ANY TIME \$100. THESE LIMITATIONS SHALL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY, AND SHALL APPLY TO THE FULLEST EXTENT PERMITTED BY LAW.

6. Hyperlinks. References or hyper-text links in the Service or the IEDR Platform to any sites, names, marks, products or services of any Authorized Party or other third party are provided solely as a convenience and do not constitute or imply E Source's endorsement or recommendation of such party or its products or services. E Source does not provide any assurances regarding third-party products or services or the content or accuracy of material on third party sites, including those of Authorized Parties. If you click on any such links and leave the IEDR Platform, you will be subject to the Authorized Party or third party's terms and conditions regarding their products and services, including their terms of service and privacy policy.

7. Governing Law. This Agreement and any dispute, proceeding, or claim of any nature arising out of or in any way relating to this Agreement shall be governed by the laws of the State of New York, without regard to its choice of law rules, and the Parties hereby irrevocably and unconditionally submit to the exclusive jurisdiction of the courts sitting in New York, New York, state and/or federal, in all matters arising out of or in any way relating to this Agreement.

8. Assignment. This Agreement shall not be transferred or assigned, in whole or in part, by you without the prior written consent of E Source. E Source may transfer its rights and obligations under this Agreement in conjunction with (i) a sale of all or substantially all of its assets or equity, or (ii) a merger or similar transaction; provided that the acquiring or resulting entity agrees in writing to be bound by this Agreement. Any purported assignment in violation of this Section is void.

9. Miscellaneous. If any provision of this Agreement is found to be illegal or unenforceable, the other provisions shall remain effective and enforceable to the greatest extent permitted by applicable law. Failure to enforce any provision of this Agreement shall not constitute a waiver of any term hereof. All notices must be in writing and sent to the other Party through the contact information provided. Any notice shall be transmitted in person, by commercial overnight courier, or by registered or certified US mail, return receipt requested. Notices shall be deemed effective upon receipt. Nothing shall be construed as creating a partnership, joint venture, agency or any other relationship. This Agreement is not made for, and shall not benefit or create any right or cause of action in favor of or for the benefit of, any person or entity other than E Source and you. This Agreement embodies the entire understanding between the Parties regarding its subject matter and supersedes any and all prior understandings, arrangements, and agreements, whether

oral or written, relating to the subject matter hereof. Other than E Source's updates to the Terms of Use or Privacy Policy as set forth therein, or updates required by law, this Agreement shall not be modified or amended except by a written document executed by both Parties.

Attachment 4- DATA SECURITY AGREEMENT

This Data Security Agreement (“Agreement”) by and between E Source Companies LLC (E Source) and the entity identified as the Energy Services Entity (“ESE”) to obtain data services. This Agreement is effective as of the day ESE checks a box indicating its agreement with the terms of this Agreement (the “Effective Date”).

BY CHECKING A BOX AND CLICKING “AGREE”, YOU ARE INDICATING YOUR ACCEPTANCE OF THIS AGREEMENT, AND YOUR AGREEMENT TO THE TERMS OF THIS AGREEMENT. BY INDICATING YOUR ACCEPTANCE TO THIS AGREEMENT, YOU REPRESENT THAT YOU ARE A REPRESENTATIVE OF ESE AND HAVE THE AUTHORITY TO BIND ESE TO THE TERMS AND CONDITIONS IN THIS AGREEMENT, INCLUDING WITH RESPECT TO YOU AND ALL ESE USERS. IF YOU DO NOT HAVE SUCH AUTHORITY, YOU MUST NOT ACCEPT THIS AGREEMENT AND MAY NOT USE THE SERVICES.

RECITALS

WHEREAS, the New York State Public Service Commission (“PSC” or “Commission”) in its February 11, 2021 *Order Implementing an Integrated Energy Data Resource* (“IEDR”) in Case 20-M-0082 (the “IEDR Order”), directed the electric and gas investor-owned utilities to work with Department of Public Service Staff and the New York State Energy Research and Development Authority (“NYSERDA”), and other stakeholders in the development and implementation of a statewide, centralized repository to collect, integrate, analyze, and manage a wide variety of standardized energy-related information from the State’s utilities and other sources (the “IEDR Platform”), to provide Energy Service Entities with access to certain Confidential Customer Information;

WHEREAS, the Commission, in the April 15, 2021 *Order Adopting a Data Access Framework (DAF) and Establishing Further Process*, (the “DAF Order”) adopted a Data Access Framework that serves as a single source for statewide access requirements and provides uniform and consistent guidance on what is needed for access to energy related data, including the availability of such data;

WHEREAS, E-Source operates the IEDR Platform, which allows parties to access certain public information, utility information, Confidential Customer Information, and other information; ESE is subject to the then-current version of the Terms of Use for the IEDR Platform.

WHEREAS, the Commission, in the October 13, 2023 *Order Addressing Integrated Energy Data Resource Matters in Case 20-M-0082*, (the “October 2023 Order”), required the IEDR to comply with all aspects of implementing and operating the IEDR and must comply with any policies adopted under the DAF;

WHEREAS, as set forth in the October 2023 Order, the Commission requires that any ESE seeking access to data via the IEDR platform to comply with the policies and requirements established as part of the DAF for release of such data, including the signing of a Data Security Agreement or Data Access Agreement between the data custodian and the ESE, which details the responsibilities of both parties in protection of said data;

WHEREAS, ESE desires to have access to Confidential Customer Information, and the Commission has ordered E-Source to provide to ESE certain Customer utility information as directed by the Customer;

WHEREAS, for ESE to access Confidential Customer Information from the IEDR Platform, E-Source and ESE are required to enter into this Agreement to establish, among other things, ESE's obligations of security and confidentiality with respect to the Confidential Customer Information in a manner consistent with the orders, rules and regulations of the Commission and requirements of E-Source; and

WHEREAS, to use certain features of the IEDR Platform, ESE must establish an account with UtilityAPI, Inc. ("UtilityAPI"), an E Source Representative. To the extent that such UtilityAPI account is used in connection with ESE's use of or access to the IEDR Platform or Confidential Customer Information, such account constitutes part of the IEDR Platform and UtilityAPI is an intended third-party beneficiary of the ESE's representations, agreements and obligations in this Agreement.

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 Customer Information" means: Customer utility information provided by E Source to ESE, other than (i) information which is or becomes generally available to the public other than as a result of a disclosure by ESE or its Representatives; (ii) information which was already known to ESE on a non-confidential basis prior to being furnished to ESE by E Source; (iii) information which becomes available to ESE on a non-confidential basis from a source other than E Source or a representative of E Source if such source was not subject to any prohibition against transmitting the information to ESE and was not bound by a confidentiality agreement with E Source; (iv) information which was independently developed by ESE or its Representatives without reference to, or consideration of, the Customer utility information provided by E Source; or (v) information provided by the Customer with Customer consent where the Customer expressly agrees that the information is public.
- b. "Customer" means a customer of a New York State utility company, the New York Power Authority, or the Long Island Power Authority.
- c. "Cybersecurity and Data Privacy Protections" refer to controls addressing the risk to IT systems and data. These cybersecurity requirements are applicable to ESE or its Third-Party Representative that electronically receive or exchange Confidential Customer Information. These controls also implement and address the risk of improper access, or misuse, of Confidential Customer Information. The data privacy protections are required of ESE if it has custody or control of, or Processes, Confidential Customer 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 Customer 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; (C) the Commission rules, regulations, and guidelines relating

to data access, Cybersecurity and Data Privacy Protections. Subject to the above, ESE will determine and implement the necessary Cybersecurity and Data Privacy Protections to be in compliance with all Commission Orders regarding Cybersecurity and Data Privacy Protections.

- e. "Data Security Incident" means a situation when E Source or ESE reasonably believes that there has been: (A) the loss or misuse (by any means) of Confidential Customer Information; (B) the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of Confidential Customer Information, or Private Information as defined by GBL § 899-aa, computer systems, networks, or devices used by ESE to Process Confidential Customer Information; (C) any other act or omission that compromises the security, confidentiality, or integrity of Confidential Customer Information, or (D) any breach of any Data Protection Requirements in relation to the Processing of Confidential Customer Information, including by any current or former Representatives. An Event is not a Data Security Incident.
- f. "E-Source Data" means data held by E-Source, whether produced in the normal course of business or at the request of ESE.
- g. "ESE" means any entity (including, but not limited to, energy service companies (ESCOs), DERS, community choice aggregation (CCA) administrators, and contractors of such entities with an electronic connection to E-Source) that provides energy or performs an energy related service and is seeking access to Confidential Customer Information.
- h. "Event" means any observable occurrence in a network or system which requires further investigation. After investigation, an Event may, or may not, be declared a Data Security Incident. "Information Security Requirements for Vendors and External Partners" means ESE's policy on information security requirements and handling of Confidential Information for ESE's representatives who provide IT products, services or support to ESE.
- i. "Information Technology" means the use of computer, telecommunications and electric distribution facilities and software for storing, retrieving, sending and processing information.
- j. "Green Button Connect" or "GBC" provides a set of standards for allowing interoperable communications of energy usage and billing information.
- k. "PSC" or "Commission" shall have the meaning attributed to it in the Recitals.
- l. "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 Customer Information or E Source 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.
- m. "Third-Party Representatives" or "Representatives" means those agents acting on behalf of ESE's that are contractors or subcontractors and that store, transmit or process Confidential Customer Information.
- n. "Services" mean any activities that transfer electronically or use Confidential Customer Information, or which utilize a direct electronic connection with E Source, where the direct electronic connection is made by ESE or its Third Party Representative.

- o. The Service Organization Control (SOC) II is an independently produced report that is an industry-standard report on controls at a service organization intended to mitigate risks related to the five trust service principles of security, availability, processing integrity, confidentiality, and privacy.
- p. “SOC II Equivalent Audit” means an audit conducted by a qualified independent cyber security entity that reviews ESE’s security data processing policies and procedures necessary to comply with this Agreement, including at minimum, strict adherence to information security policies and procedures and encompassing the security, availability, processing, integrity and confidentiality of Confidential Customer Information.

- 2. Scope of the Agreement.** This Agreement shall govern ESE’s Cybersecurity and Data Privacy Protections when it electronically receives or exchanges Confidential Customer Information and other information from E Source and the Data Protection Requirements that apply to such information disclosed to ESE or to which ESE is given access by E Source, including all archival or back-up copies of the Confidential Customer Information held or maintained by ESE (or its Representatives). No financial information, other than billing information, will be provided pursuant to this Agreement. If any information is inadvertently sent to ESE, ESE will immediately notify E Source and destroy any such information in the appropriate manner.
- 3. Governance of Confidential Customer Information and Transfer of information Electronically Exchanged by E Source with ESE.** The Parties agree that, except as otherwise permitted in this Agreement, Confidential Customer Information will not be disclosed without the customer’s consent. The Parties agree that Data Protection Requirements will govern the electronic interconnection and data transfer between the Parties. The Parties agree that Data Protection Requirements mean that ESE, at a minimum, will maintain Cybersecurity and Data Privacy Protections that are equivalent or superior to those that ESE requires of its vendors and external partners through the Information Security Requirements for Vendors and External Partners.
- 4. Customer Consent.** ESE agrees to comply with Federal, State and local laws, the orders, rules and regulations of the Commission, and applicable tariffs, regarding obtaining Customer consent before requesting Customer Confidential Information from E Source.
- 5. Provision of Information.** E Source agrees to provide to ESE or its Third-Party Representatives, certain Confidential Customer Information, as requested, provided that: (A) ESE (and its Third-Party Representatives with an electronic connection to the utility other than by email) are in compliance with the terms of this Agreement in all material respects; (B) if required by E Source due to the identification of a potential or actual Data Security Incident, ESE shall undergo a security audit, at ESE’s expense¹⁰; (C) ESE (and its Third-Party Representatives with an electronic connection to the IEDR shall have and maintain throughout the term, systems and processes in place and as detailed in the Self-Assessment to protect utility IT systems, Data Privacy Protections and Confidential Customer Information. Provided the foregoing prerequisites have been satisfied and a Customer consents to disclosure, ESE shall be permitted access to Confidential Customer Information and/or E Source shall provide such Confidential Customer Information to ESE. Nothing in this Agreement will be interpreted or construed as granting either Party any license or other right under any patent, copyright, trademark, trade secret, or other proprietary right or any right to assert any lien over or right to withhold from the other Party any data of the other Party. ESE will comply

¹⁰ An audit related to a Data Security Incident is used to verify that the necessary Cybersecurity and Data Privacy Protections are in place for E Source to provide certain Confidential Customer Information to ESE or its Third-Party Representatives with an electronic connection to the IEDR. The same audit requirements will apply as in Section 9. However, ESE will be responsible for the cost of the audit in order to be re-authorized to receive data from E Source.

with the security requirements set forth in this Agreement.

- 6. Confidentiality.** ESE shall: (A) hold all Confidential Customer Information in strict confidence, including pursuant to the terms and conditions of this Agreement. except except as otherwise expressly permitted by Section 7 herein; (B) not disclose Confidential Customer Information to any Third-Party Representatives, or affiliates, except as set forth in Section 7(a) of this Agreement; (C) not Process Confidential Utility Information other than as directed by a Customer; (D) limit reproduction of Confidential Customer Information; (E) store Confidential Customer Information in a secure fashion at a secure location that is not accessible to any person or entity not authorized to receive the Confidential Customer Information under the provisions hereof; (F) otherwise use at least the same degree of care to avoid publication or dissemination of the Confidential Customer 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, E Source shall have the right for cause to request reasonable further assurances that the foregoing restrictions and protections concerning Confidential Customer Information are being observed and ESE shall be obligated to promptly provide E Source with the requested assurances. ESE may provide Confidential Customer Information to a Third-Party representative without a direct electronic connection with E Source, 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.

E-Source will keep confidential the registration information provided by ESE for access to the IEDR Platform.

7. Exceptions Allowing Disclosure of Confidential Information.

- a. Disclosure to Representatives.** Notwithstanding the provisions of Section 6 herein, ESE may disclose Confidential Customer Information to its Third-Party Representatives who have a legitimate need to know or use such Confidential Customer Information for the purposes of providing Services in accordance with the Commission order and rules, provided that each such Third-Party Representative first is advised by ESE of the sensitive and confidential nature of such Confidential Customer Information. ESE shall require its Representatives to comply with the Information Security Requirements for Vendors and External Partners prior to disclosure of Confidential Customer Information and 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 ESE 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 Customer 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), ESE shall, except to the extent prohibited by law, within one (1) business day, notify E Source, in writing, of the pending or threatened compulsion. To the extent lawfully allowable, the Parties shall each have the independent 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 Customer 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 Customer Information that must be disclosed. In any event, ESE and its Third-Party Representatives shall disclose only such Confidential Customer 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 ESE and its Third-Party Representatives shall use all reasonable efforts to ensure that all Confidential Customer Information that is so disclosed will be accorded confidential treatment.

8. Return/Destruction of Information. Within thirty (30) days after E-Source's written demand, ESE shall (and shall cause its Third-Party Representatives to) cease to access and Process Confidential Customer Information and shall at E-Source's option: (A) return such Confidential Customer Information to E-Source in such manner, format, and timeframe as reasonably requested by E-Source or, if not so directed by E-Source, (B) shred, permanently erase and delete, degauss or otherwise modify so as to make unreadable, unreconstructible and indecipherable ("Destroy") all copies of all Confidential Customer Information (including any and all extracts, compilations, studies, or other documents based upon, derived from, or containing Confidential Customer Information) that has come into ESE's or its Third-Party Representatives' possession, including Destroying Confidential Customer 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 Customer Information by ESE and its Third-Party Representatives shall cease, provided any items required to be maintained to meet reporting requirements as set forth by federal, state, and/or local laws, regulations, rules, NY state policies, or executive directives, by governmental administrative rule or law or necessary for legitimate legal needs will not be destroyed until permitted and will remain subject to confidentiality during the retention period. If E-Source requires the return or destruction of Confidential Customer Information, E-Source will specify the reason for the demand. ESE agrees that upon a Customer revocation of consent, ESE warrants that it will no longer access Confidential Customer Information and that it will Destroy any Confidential Customer Information of that Customer in its or its Third-Party Representative's possession. Notwithstanding the foregoing, ESE and its Third-Party Representatives shall not be obligated to erase Confidential Customer 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 Cybersecurity and Data Privacy Protections and Data Protection Requirements to limit access to or recovery of Confidential Customer Information from such computer backup system and; (3) keep all such Confidential Customer Information confidential in accordance with this Agreement. ESE shall, upon request, certify to E-Source 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 E-Source 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 Customer Information pursuant to this Section may occur if the E-Source has been notified of a potential or actual Data Security Incident and E-Source has a reasonable belief of potential ongoing harm or the Confidential Customer Information has been held for a period in excess of its retention period. The obligations under this Section shall survive any expiration of termination of this Agreement.

9. Audit. Upon thirty (30) days' notice to ESE ESE shall permit an auditor selected by E Source to audit and inspect, at E-Source'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 E Source's regulators or if there has been a Data Security Incident). The audit may include (A) the facilities of ESE and ESE's Third-Party Representatives where Confidential Customer Information is Processed by or on behalf of ESE; (B) any computerized or paper systems used to Process Confidential Customer 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 Customer Information. Such audit

rights shall be limited to verifying ESE's compliance with this Agreement, including all applicable Data Protection Requirements. If ESE provides a SOC II report or its equivalent (current within twelve (12) months of the E Source's request) to E Source, or commits to complete an independent third-party audit of ESE's compliance with this Agreement acceptable to E Source at ESE's sole expense, within one hundred eighty (180) days, no audit by an auditor selected by E Source is necessary absent a Data Security Incident. Any audit must be subject to confidentiality and non-disclosure requirements set forth in Section 6 of this Agreement. The auditor will audit the ESE's compliance with the required Cybersecurity and Data Privacy Protections and provide those results to E Source and ESE. In the event of a "failed" audit dispute, dispute resolution may proceed through mediation with a third-party mediator agreed to by the Parties. ESE shall, within thirty (30) days, or within a reasonable time period agreed upon in writing between ESE and E Source, correct any deficiencies identified in the audit, and provide the SOC II audit report or its equivalent or the report produced by the independent auditor at ESE expense to E Source and provide a report regarding the timing and correction of identified deficiencies to E Source.

10. Investigation. Upon notice to ESE, ESE shall assist and support E Source in the event of an investigation by any regulator or similar authority, if and to the extent that such investigation relates to Confidential Customer Information Processed by ESE on behalf of E Source. Such assistance shall be at E Source'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 Customer Information that is Processed by, or on behalf of, ESE. ESE shall investigate all detected Events and shall notify E Source in writing as soon as possible upon declaration of a Data Security Incident and in accordance with the New York State Information Security Breach and Notification Act, and applicable laws, rules, and regulations. ESE will notify E Source if ESE determines that there is a potential or actual unauthorized disclosure of Confidential Customer Information and/or potential or actual harm to E Source Information Technology or Operation Technology systems. ESE will immediately take all necessary steps to eliminate or contain any exposure of Confidential Customer Information and keep E Source 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 E Source and/or E Source'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 E Source 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 E Source 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 E Source's approval, which approval will not be unreasonably withheld, that reduces the likelihood of a recurrence of such Data Security Incident. ESE agrees that E Source may at its discretion and without penalty immediately suspend performance hereunder and/or terminate the Agreement if a Data Security Incident occurs and it has a reasonable belief of potential ongoing harm. Any suspension made by E Source 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 E Source so that E Source IT systems and Confidential Customer Information are safe and the ESE is capable of maintaining adequate security once electronic communication resumes. Actions made pursuant to this paragraph, including a suspension will be subject to dispute resolution and appeal as applicable.

12. 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 E Source, and ESE shall acquire no

ownership interest in the Confidential Customer Information. No rights or obligations other than those expressly stated herein shall be implied from this Agreement.

13. Additional Obligations.

- a. ESE shall not create or maintain data which are derivative of Confidential Customer Information except for the purpose of performing its obligations under this Agreement, or after obtaining Customer consent, for meeting reporting requirements as set forth by federal, state, and/or local laws, regulations, rules, NY state policies, or executive directives, or as expressly authorized by the Customer, unless that use violates Federal, State, and local laws, tariffs, rules, and regulations. For purposes of this Agreement, the following shall not be considered Confidential Customer 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, regulatory reporting, or other legitimate business purposes; 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 E Source in violation of any privacy or security law known by ESE to be applicable to E Source.
- 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 as reasonably determined by E Source in its discretion, to protect the security of Confidential Customer 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 Customer 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.
- d. ESE and E Source shall safely secure or encrypt during storage and encrypt during transmission all Confidential Customer 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 E Source 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 Customer Information Processed by ESE to the extent such request, complaint or other communication relates to ESE's Processing of such individual's Confidential Customer Information.
- f. ESE shall establish policies and procedures to provide all reasonable and prompt assistance to E Source 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 Customer Information, data theft, or other unauthorized release of Confidential Customer Information, disclosure of Confidential Customer Information, or misuse of Confidential Customer Information to the extent such request, complaint or other communication relates to ESE's accessing or Processing of such Confidential Customer Information.
- g. ESE will not process Confidential Customer Information outside of the United States absent a

written agreement, whereby ESE shall require its Third Party Representatives to comply with both the Data Protection Requirements and ESE's Information Security Requirements for Vendors and External Partners. For the avoidance of doubt, Confidential Customer Information stored in the United States will be maintained in a secure fashion at a secure location pursuant to the terms and conditions of this Agreement.

14. Specific Performance. The Parties acknowledge that disclosure or misuse of Confidential Customer Information in violation of this Agreement may result in irreparable harm to E Source, the amount of which may be difficult to ascertain and which may not be adequately compensated by monetary damages, and that therefore E Source shall be entitled to specific performance and/or injunctive relief to enforce compliance with the provisions of this Agreement. E Source'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 Customer Information hereunder. Each Party agrees to waive any requirement for the securing or posting of any bond or other security in connection with E Source obtaining any such injunctive or other equitable relief.

15. Indemnification.

To the fullest extent permitted by law, ESE shall indemnify and hold E Source, UtilityAPI, Inc., each of their affiliates, and their respective officers, directors, trustees, shareholders, employees, and agents, and the Utility from which the Confidential Customer Information originated, 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, including allowing unauthorized access to or disclosure of Confidential Customer Information or improper use or misuse of same, except to the extent that the loss, cost, damage or expense is caused by the negligence, gross negligence, or willful misconduct of E Source.

16. 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.

17. Term and Termination. This Agreement shall be effective as of the ESE registration date (i.e., the date ESE clicks "Agree" or "I Accept" to this Agreement) and shall remain in effect until terminated either Party 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. Further, either party may dispense with the required thirty (30) day notice period in the event of a material breach hereof by ESE or its Third-Party Representatives. For the purpose of clarity, a breach of Sections 3-4, 6-11, 13, 14, 15, 16, and 23 shall be a material breach hereof. The Breaching Party will provide the non-breaching Party with a written description and notice of material breach. Upon the expiration or termination hereof, neither ESE nor its Third-Party Representatives shall have any further right to Process Confidential Customer

Information, unless the Customer has given written or electronic consent to do so, and shall immediately comply with its obligations under Section 8 Upon expiration or termination of this Agreement, ESE shall retain the right to Process all Confidential Customer Information acquired during the term of this Agreement to meet reporting requirements as set forth by federal, state, and/or local laws, regulations, rules, NY state policies, or executive directives.

- 18. Consent to Jurisdiction; Selection of Forum.** ESE irrevocably submits to the jurisdiction of the Commission and courts located within the State of New York with regard to any dispute or controversy arising out of or relating to this Agreement. ESE agrees that service of process on it in relation to such jurisdiction may be made by certified or registered mail addressed to ESE and that such service shall be deemed sufficient even under circumstances where, apart from this Section, there would be no jurisdictional basis for such service. ESE agrees that service of process on it may also be made in any manner permitted by law. The Parties agree to submit all disputes to a court of competent jurisdiction within New York or the federal courts within any County in New York as the exclusive forums for any legal or equitable action or proceeding arising out of or relating to this Agreement.
- 19. Governing Law.** This Agreement shall be interpreted, and the rights and obligations of the Parties determined in accordance with the laws of the State of New York, without recourse to such state's choice of law rules, exclusive of its choice of law provisions.
- 20. Survival.** The obligations of ESE under this Agreement shall continue so long as ESE and/or ESE's Third-Party Representatives continue to have access to, are in possession of or acquire Confidential Customer Information even if all Agreements between ESE and Utility have expired or been terminated.
- 21. 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 electronic consent to the terms of this Agreement, including any such copies delivered electronically as a .pdf file, shall be treated for all purposes as originals.
- 22. Amendments; Waivers.** 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.
- 23. Assignment.** This Agreement (and E Source's or ESE's obligations hereunder) may not be assigned by ESE or Third-Party Representatives without the prior written consent of E Source, and any purported assignment without such consent shall be void. Consent will not be unreasonably withheld.
- 24. Severability.** Any provision of this Agreement which is determined by any court or regulatory body or 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.
- 25. Entire Agreement.** This Agreement (including any Exhibits hereto) constitutes the entire Agreement between the Parties with respect to the subject matter hereof and this Agreement may not be amended without the written Agreement of the Parties.
- 26. Third-Party Beneficiaries.** This Agreement 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, UtilityAPI, and the indemnified parties named herein, and no other party shall have any right, claim, or action as a result of this Agreement.

- 27. 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.
- 28. Relationship of the Parties.** E Source 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.
- 29. Construction.** This Agreement shall be construed as to its fair meaning and not strictly for or against any party.

SELF-ATTESTATION OF Cybersecurity Protections

The Cybersecurity protections listed below are required before ESE will be allowed access to or electronically exchange Confidential Customer Information with E Source.

WHEREAS, ESE desires to obtain or retain access to and electronically exchange Confidential Customer Information (as defined in this Data Security Agreement) with E Source, ESE must THEREFORE self-attest to ESE's compliance with the Cybersecurity Protections ("Requirements") as listed herein. ESE acknowledges that non-compliance with any of the Requirements may result in the termination of utility data access as per the discretion of E Source.

- _____ An information security policy is implemented across ESE's corporation which includes officer level approval.
- _____ An incident response procedure is implemented that includes notification as soon as possible following declaration of an incident alerting utility when Confidential Customer Information is potentially exposed, or of any other potential security breach.
- _____ Role-based access controls are used to restrict system access to authorized users and limited on a need-to-know basis.
- _____ Multi-factor authentication is used for all remote administrative access, including, but not limited to, access to production environments.
- _____ All production systems are properly maintained and updated to include security patches on a periodic basis. Where a critical alert is raised, time is of the essence, and patches will be applied as soon as practicable.
- _____ Antivirus software is installed on all servers and workstations and is maintained with up-to-date signatures.
- _____ All Confidential Customer Information is encrypted in transit utilizing industry best practice encryption methods.
- _____ All Confidential Customer Information is secured or encrypted at rest utilizing industry best practice encryption methods, or is otherwise physically secured.
- _____ It is prohibited to store Confidential Customer 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 Customer Information is stored in the United States only, including, but not limited to, cloud storage environments and data management services.
- _____ ESE monitors and alerts its network for anomalous cyber activity on a 24/7 basis.
- _____ Security awareness training is provided to all personnel with access to Confidential Customer Information.
- _____ Employee background screening occurs prior to the granting of access to Confidential Customer Information.
- _____ Replication of Confidential Customer Information to non-company assets, systems, or locations is prohibited.

_____ Access to Confidential Customer Information is revoked when no longer required, or if employees separate from ESE or its 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 indicated below.

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Attachment 5- IEDR Green Button ESE Onboarding Process

Introduction.....	38
Step 1: Begin registration with IEDR’s Green Button Connect tool	38
Step 2: Fill out the IEDR Third Party Registration form.....	39
Contact Information	39
Scope of Use Disclosure	40
Directory Listing.....	41
Terms and Conditions.....	41
Step 3: Complete the prerequisite tasks	42
Verify Email	43
Register with DPS.....	43
Agree to Terms of Service	43
Step 4: IEDR Admin approval.....	44
Step 5: Third Party is notified via email that they are “Live”	44
Existing Users	44

1 Introduction

This document summarizes the user flow for an Energy Service Entity (ESE) registering to use the IEDR’s Green Button Connect tool. To request and obtain customer data from New York’s IEDR, an ESE must register both with the IEDR platform and the New York State Department of Public Service (DPS). In the series of images below, we detail how a new user would make their way through the IEDR Third Party registration process.

2 Step 1: Begin registration with IEDR’s Green Button Connect tool

From [the Green Button Connect homepage](#), users will find a section named “For Third Parties” and a button labeled “Register”. By clicking the “Register” button, an ESE will arrive at the [registration page](#) intended for first time users.

New York State's Integrated Energy Data Resource (IEDR) New York State Integrated Energy Data Resource

Home EIAI Rate Plans Green Button About Connect With Us

⚠ This system is a **sandbox deployment**, for testing purposes only. Some functionality may change when the full version goes live.

Green Button Home Directory My Authorizations Help

Securely request or share utility data

The Integrated Energy Data Resource Program (IEDR) is using [Green Button Connect](#), a data standard to provide residential and business energy customers with more choice in how you access your utility data. Green Button applications can analyze this data to provide customers with personalized ways to increase energy efficiencies. This will help customers save money on their monthly bills and reduce demand on the energy system. All you need to do is click below to get started.

Utilities that participate in this program are Central Hudson, Consolidated Edison, Liberty Utilities, National Fuel, National Grid, New York State Electric & Gas, Orange & Rockland, PSEG Long Island, and Rochester Gas and Electric.

For Third Party Providers

→

Register

Already registered? Go to your [dashboard](#)

Third Parties who wish to be registered and showcased as an available partner in IEDR's Green Button directory will be required to submit a registration form.

For Customers

Browse the Directory

The Green Button Connect My Data (CMD) standard allows utility customers to authorize direct, secure transfer of their energy usage data to third parties that can assist them with ways to potentially manage and conserve energy.

Questions?

Contact Support

Or email support@iedr.utilityapi.net

3 Step 2: Fill out the IEDR Third Party Registration form

New users will be prompted to fill out the [IEDR Third Party Registration form](#) that contains four sections as discussed below.

3.1 Contact Information

When this form is submitted, an account will be created for the registrant. These fields will be used to create that user's profile and allow them to manage their profile settings and work with sample or live data authorizations with customers.



Integrated Energy Data Resource

IEDR Third Party Registration

This is where you can register as a third party for the [Integrated Energy Data Resource \(IEDR\) platform](#), so you can request data from utility customers across New York State.

To register, please fill out the fields below so we know who you are and how to get in contact with you. When you register we'll create an account on the IEDR platform where you can login and see your customer-authorized data. All fields are required.

First Name

e.g. Ben

Last Name

e.g. Wilson

Company Email

e.g. bwilson@example.com

Company Name

e.g. Example Company

Company Website

e.g. https://example.com

Password

Retype Password

Already registered? [Log in here](#)

3.2 Scope of Use Disclosure


When seeking data authorizations with utility account holders, the third party must disclose a default scope of use. This is a short statement that will be presented to customers when authorizing data sharing with this entity. After registration, the third party can modify or add additional scopes of use for their needs (with IEDR admin approval).

Scope of Use Disclosure

When you ask a customer to authorize access to their utility data, we require that you disclose how you're going to use it. Your scope of use description below will be shown to your customers on the authorization form.

Scope of Use Description 

e.g. We will use the data to calculate your solar quote.

Scope of Use Terms URL (optional) 


e.g. <https://companyname.com/data-use/terms>

NOTE: Customers will see what you write here as part of the authorization process, so try to make it easy for them to understand. You can also add more scopes of use after you register if you need more than one for different use cases.

3.3 Directory Listing

This provides the registrant with the option to be displayed in a [public directory](#) on the IEDR Green Button Connect platform. This preference and other personalization settings can be modified by the third party once registered.

Directory Listing

Integrated Energy Data Resource Program has a [public directory](#)  where you can be listed as a registered third party. You can choose to automatically be listed in this directory when your registration is approved and switched to live status. You can always change this later in your settings.

Yes, automatically list me in the public directory when approved.

3.4 Terms and Conditions

A registrant must acknowledge the [IEDR Terms of Use, as adopted by the New York Public Service Commission \(Commission\)](#), to create an account (additional terms, which may require more research and review, are not required at this initial stage).

Terms and Conditions

You must agree to use the data sharing program within our terms of service, and you must agree to use UtilityAPI's platform within its terms of service.

I have read and agree to the [IEDR Platform Terms of Use](#).

Register

[Cancel](#)

When you submit, your registration will be set in "sandbox" mode, which means you'll only be able to request data from demo accounts for testing. We'll review your registration and then email you when we switch you to "live" mode (i.e. when you can start requesting data from real customers in New York State).

4 Step 3: Complete the prerequisite tasks

With the entity now registered as an IEDR Third Party, the user can adjust their profile settings, work with sample datasets, and experience the platform in a sandbox capacity. Before a third party can be considered “review ready” by the IEDR admin team (and, upon approval, enter data sharing agreements with utility customers), they must complete three additional steps.

Integrated Energy Data Resource Program (IEDR) Settings

Registration Details

Utility: ⓘ Integrated Energy Data Resource Program [website](#) [terms](#) [docs](#)

Status: ⓘ **Sandbox** ✎

Onboarding Progress: ⓘ **Register Email on the NYS Department of Public Service Page**

This is the current progress of your onboarding with the IEDR. It governs whether you can move from sandbox to higher modes. See below for the possible steps of onboarding.

Onboarding Progress Steps:

- **Verify Email** - This step means you need to verify your email address with the IEDR. You can do so by clicking on the [Verify Email](#) link to initiate the process.
- **Register Email on the NYS Department of Public Service Page** - This means that you need to complete the appropriate business application with the [Department of Public Service](#) and include a valid email address. The domain of the registered email address will be used to verify your application.
- **Complete** - This step means you have successfully completed onboarding with the IEDR and no further action is required before moving to higher modes.

You can complete each step in any order you want, but all are required to move out of sandbox mode.

4.1 Verify Email

The third party must be able to verify the email address tied to their registered profile. By initiating the process, a verification email will be sent for the user to then act on. If the email address is ever changed by the third party in the future, this process will need to be repeated.

4.2 Register with DPS

All entities approved by the IEDR Green Button Connect tool must also be registered with the New York State Department of Public Service (DPS). In the platform's documentation, we direct registrants to the proper government sites where the specific information related to gaining and maintaining DPS registration status is better detailed.

Once registered with the DPS, either at the time IEDR Third Party registration occurs or when the third-party's name first appears on the published *Registered ESE Listing*, the automation behind the IEDR Green Button Connect tool will look to match entities across lists. If there is a direct match (or if an IEDR administrative override is implemented to accommodate an exemption such as the need to meet another Commission requirement), then the IEDR Third Party entity will satisfy the requirement. Upon regular refreshes, if this relevant record is no longer present on the DPS list, then this process must be repeated.

Third Party Registration

New York State Registration

Third Parties must be registered with New York State Department of Public Service (DPS) in addition to registering with the IEDR platform prior to being granted access to live data. For instructions on registering with DPS, see the links below. Note that the registration forms and points of contact are unique to the category of third party seeking registration.

- For Distributed Energy Resource (DER) Providers: <https://dps.ny.gov/distributed-energy-resource-der-regulation-and-oversight>
- For Energy Service Companies (ESCOs): <https://dps.ny.gov/energy-services-company-esco-competitive-market-information>
- For Energy Brokers and Energy Consultants: <https://dps.ny.gov/energy-broker-and-energy-consultant-registration>

A valid email must be supplied with the above registration that matches the email provided below on the IEDR Registration Form. If you are a third party that previously registered with DPS but did not provide a valid email address, please resubmit your registration form including only the contact details (page 1) and there will be an accelerated review and update process handled by DPS.

To confirm your registration with DPS and the presence of a valid email, check the consolidated DPS Registration Directory:

1. Navigate to: <https://documents.dps.ny.gov/PTC/home>
2. Click Dataset on the footer of this page
3. Click Download on the "Registered ESE Listing (.csv)" menu option

4.3 Agree to Terms of Service

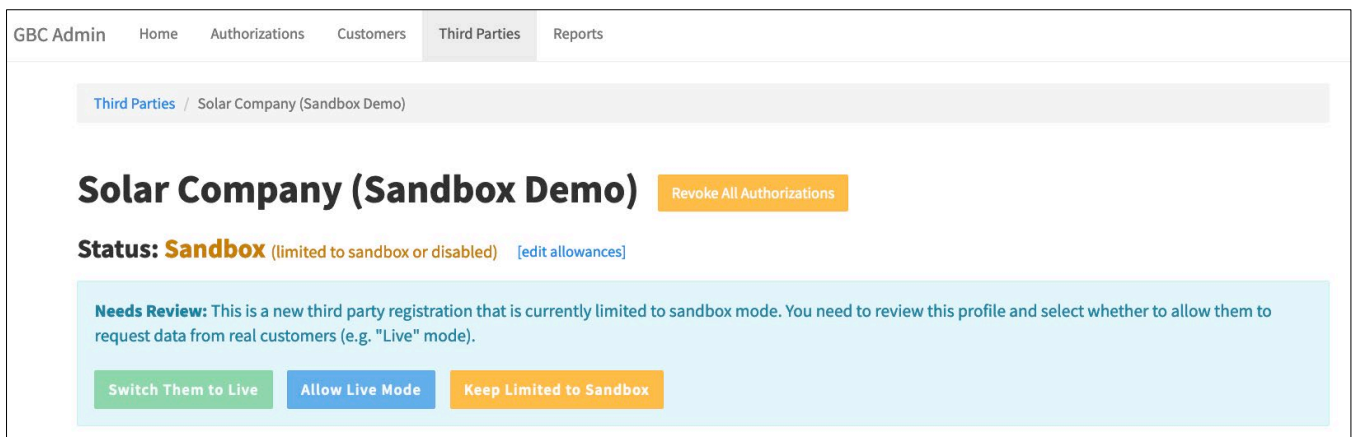
It is anticipated that the IEDR User Agreement, Data Sharing Agreement and Self-Attestation of Cybersecurity Protections will be presented to an ESE in a separate window of terms as part of this step. The responses to these fields will be logged and reviewable by the IEDR admins.

Note: This specific functionality has not been, and will not be, released without finalized terms approved by the Commission.

5 Step 4: IEDR Admin approval

Once the prior conditions are met, the IEDR admin team will be notified that an entity has transitioned to a “review ready” state. The IEDR admin team will perform a final review of the profile, and if all requirements are met, switch them into “live mode”.

If a profile does not meet the standards required by the IEDR admin team, then these profiles can be kept in “sandbox mode” or can be set as “disabled”.



GBC Admin Home Authorizations Customers Third Parties Reports

Third Parties / Solar Company (Sandbox Demo)

Solar Company (Sandbox Demo) [Revoke All Authorizations](#)

Status: **Sandbox** (limited to sandbox or disabled) [\[edit allowances\]](#)

Needs Review: This is a new third party registration that is currently limited to sandbox mode. You need to review this profile and select whether to allow them to request data from real customers (e.g. "Live" mode).

[Switch Them to Live](#) [Allow Live Mode](#) [Keep Limited to Sandbox](#)

6 Step 5: Third Party is notified via email that they are “Live”

Once approved by an IEDR admin, an email notification will be sent out to notify the profile that they are now in “live mode”. This allows the third party to complete data sharing agreements with utility customers through the Green Button Connect platform.

7 Existing Users

Previously registered users will be able to access the dashboard any time after registration and will be able to:

- Bookmark the dashboard site once first directed there upon registration
- Use the link provided in the registration confirmation email
- Follow the “*Already registered? Go to your [dashboard](#)*” prompt from the Green Button Connect homepage
- If on the registration page, there are prompts asking “*Already registered? [Log in here](#)*”