# AVANGRID Privacy and Data Security Rider

For the purposes of this Privacy and Data Security Rider (the "Rider") [ ][1] and any of its affiliates procuring or receiving services, works, equipment or materials under the Agreement (as defined below) shall be hereinafter referred to as the "CUSTOMER". [ ][2] shall be hereinafter referred to as the "VENDOR"

(a) Among other, the purpose of this Rider is to enable the VENDOR to Process on behalf of the CUSTOMER the Personal Data and Company Data necessary to comply with the purpose of the Agreement (as defined below), define the conditions under which the VENDOR will Process the Personal Data and Company Data to which it has access during the performance of the Agreement, and establish the obligations and responsibilities of the VENDOR derived from such Processing. Personal Data disclosed by CUSTOMER to VENDOR is provided only for limited and specified purposes as set forth in the Agreement and this Rider.

(b) The following definitions are relevant to this Rider:

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

(ii) "Company Data" means any and all information concerning CUSTOMER and its affiliates and their respective business in any form, or to which the CUSTOMER or its affiliates have access, that requires reinforced protection measures, including but not limited to CUSTOMER sensitive information (confidential or restricted), internal use information, Personal Data, Cardholder Data, commercially sensitive information, Critical Infrastructure Information, other information that relates to critical infrastructure, information that relates to the operation or functionality of facilities, networks, or grids, commercially sensitive information, strategic business information, credentials, encryption data, system and application access logs, or any other information that may be subject to legal or regulatory requirements.

(iii) "Critical Infrastructure Information" means engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure (physical or virtual) that (A) relates details about the production, generation, transmission, or distribution of energy; (B) could be useful to a person planning

[1] Insert the name of the Avangrid entity that is the signatory of the Agreement.
[2] Insert the name of the Vendor that is the signatory of the Agreement.



Take care of the environment.
Printed in black and white and only if necessary.

# AVANGRID Privacy and Data Security Rider

an attack on critical infrastructure; (C) is exempt from mandatory disclosure under the Freedom of Information Act; and (D) gives strategic information beyond the location of the critical infrastructure.

(iv) "Processing" (including its cognate, "process") means any operation, action, error, omission, negligent act, or set of operations, actions, errors, omissions, or negligent acts that is performed upon Personal Data or Company Data, whether or not by automatic means, including, without limitation, collection, recording, organization, storage, access, adaptation, alteration, retrieval, consultation, retention, use, disclosure, dissemination, exfiltration, taking, removing, copying, making available, alignment, combination, blocking, deletion, erasure, or destruction.

(v) "Data Security Incident" means: (A) the loss or misuse (by any means) of Personal Data or Company Data; (B) the inadvertent, unauthorized and/or unlawful Processing, corruption, modification, transfer, sale or rental of Personal Data or Company Data; (C) any other act, omission or circumstance that compromises or may reasonably compromise the security, confidentiality, or integrity of Personal Data or Company Data, including but not limited to incidents where Personal Data or Company Data has been damaged, lost, corrupted, destroyed, or accessed, acquired, modified, used, or disclosed by any unauthorized person, by any person in an unauthorized manner, or for an unauthorized purpose; (D) any act, omission or circumstance that compromises or may reasonably compromise the cybersecurity of the products and services provided to CUSTOMER by VENDOR or the physical, technical, administrative, or organizational safeguards protecting VENDOR's systems or, if VENDOR knows or reasonably believes, CUSTOMER's systems storing or hosting Personal Data or Company Data, or (F) VENDOR receives any complaint, notice, or communication which relates directly or indirectly to (x) VENDOR's Processing of Personal Data or Company Data or VENDOR's compliance with Technical and Organizational Measures or applicable law in connection with Personal Data or Company Data or (y) the cybersecurity of products and services provided to CUSTOMER by VENDOR.

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

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

(viii) "Agreement" shall mean the [ ][3] dated as

[3] Insert the name of the agreement. For example, Master Service Procurement Agreement.



Take care of the environment.
Printed in black and white and only if necessary.

# AVANGRID Privacy and Data Security Rider

of [_____][4] and any purchase orders, statements of work, notice to proceed and related documents issued in connection therewith.

(c) Personal Data and Company Data shall at all times remain the sole property of CUSTOMER, and nothing in this Rider or the Agreement will be interpreted or construed as granting VENDOR any license or other right under any patent, copyright, trademark, trade secret, or other proprietary right to Personal Data or Company Data. VENDOR shall not create or maintain data which are derivative of Personal Data or Company Data except for the purpose of performing its obligations under the Agreement and this Rider and as authorized by CUSTOMER.

(d) Regarding the Processing of Personal Data and Company Data, the parties agree that:

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

(ii) The parties agree that:

- The Processing activities that will be carried out by VENDOR are: [_____].[5]

- The categories of Personal Data or Company Data that will be Processed by VENDOR are: [_____].[6]

[4] Insert date of the agreement.
[5] Insert Processing activities to be carried out by Vendor. How will the third party access the data? What type of actions will the third party perform with the data?
[6] Insert categories of Personal Data. Please review Data Classification Rule. With respect to Personal Data, include a listing of personal data elements or categories that will be processed.



Take care of the environment.
Printed in black and white and only if necessary.

# AVANGRID Privacy and Data Security Rider

- The categories of Personal Data subjects whose information will be processed by VENDOR are: [_____].[7]

- The instructions for the Processing of Personal Data or Company Data are: [_____].[8]

- The duration of the Processing shall be: [_____].[9]

(iii) VENDOR shall immediately inform the CUSTOMER if in VENDOR's opinion a Processing instruction given by CUSTOMER may infringe the privacy and security laws applicable to VENDOR's services or VENDOR's possession or Processing of Personal Data or Company Data.

(iv) In the event that the activities to be carried out by VENDOR under the Agreement do not require access to Personal Data, VENDOR, its employees and representatives shall be prohibited from accessing and Processing Personal Data. If they gain access to Personal Data, VENDOR shall immediately inform CUSTOMER. Notwithstanding the foregoing, any Processing of Personal Data by VENDOR shall be subject to the terms and conditions set forth in this Rider.

(e) As a condition to starting work, VENDOR's employees and other persons authorized, pursuant to the terms of this Rider, to Process Personal Data or Company Data shall acknowledge in writing their agreement to [(i) comply with the terms of CUSTOMER's Acceptable Use Requirements set forth in Schedule C hereto, as such Acceptable Use Requirements may be modified or supplemented from time-to-time upon notice from the CUSTOMER,][10] (ii) maintain the confidentiality of Personal Data and Company Data, and (iii) comply with any applicable Technical and Organizational Measures. In addition, VENDOR's employees and other authorized persons that access CUSTOMER's premises shall abide by CUSTOMER's physical security policies, rules and procedures.

(f) At any and all times during which VENDOR is Processing Personal Data or Company Data, VENDOR shall:

(i) Comply with all applicable privacy and security laws to which it is subject, or that are applicable to VENDOR's services or VENDOR's possession or Processing of Personal Data and\or Company Data, and not, by act or omission, place CUSTOMER or its affiliates in violation of any privacy or security law known by VENDOR to be applicable to them;

(ii) With regards to the Processing of Personal Data, maintain a record of Personal Data Processing activities carried out on behalf of CUSTOMER, which shall include at least:

---

[7] Insert categories of data subjects.
[8] Insert instructions.
[9] Insert duration.
[10] The Acceptable Use Requirements only need to be included if the VENDOR will be using Avangrid information resources or will have access the Avangrid information technology environment.



Take care of the environment.
Printed in black and white and only if necessary.

# AVANGRID Privacy and Data Security Rider

(A) The name and contact details of the VENDOR, any subcontractor, where applicable and as previously authorized by CUSTOMER, the CUSTOMER on whose behalf the VENDOR is Processing Personal Data, their respective representatives and, where applicable, the data protection officer;

(B) The categories of Processing activities carried out on behalf of CUSTOMER;

(C) Where applicable, international transfers of Personal Data to a third country or international organization, identifying the third country or international organization, and identification of appropriate safeguards;

(D) A general description of the appropriate Technical and Organizational Measures that VENDOR is implementing relating to:

- The ability to ensure the continued confidentiality, integrity, availability and resilience of Personal Data Processing systems and services;

- The ability to quickly restore availability and access to Personal Data in the event of a physical or technical incident; and

- A process of regular verification, evaluation and assessment of the effectiveness of Technical and Organizational Measures to ensure the security of the Personal Data Processing;

- Pseudonymization and encryption of Personal Data;

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

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

(B) Quickly restore availability and access to Personal Data and Company Data in the event of a physical or technical incident;



Take care of the environment.
Printed in black and white and only if necessary.

# AVANGRID Privacy and Data Security Rider

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

(D) Pseudonymize and encrypt Personal Data, where applicable; and

(E) Safely secure or encrypt all Personal Data and Company Data, during storage or transmission;

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

(v) Notify CUSTOMER at asoc@avangrid.com or (855)548-7276[11] no later than one (1) day from the date of obtaining actual knowledge of any Data Security Incident, or from the date the VENDOR reasonable believes that a Data Security Incident has taken place, whatever is earlier, and at VENDOR's cost and expense, assist and cooperate with CUSTOMER concerning any disclosures to affected parties and other remedial measures as requested by CUSTOMER or required under applicable law. If the Data Security Incident involves Personal Data, the following information shall be provided as a minimum:

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

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

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

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

(vi) VENDOR designates the following contacts for the purposes of communications related to a Data Security Incident: [__ Insert name and phone number _].[12]

(vii) Assist and cooperate with CUSTOMER to enable CUSTOMER to comply with its

[11] Include Avangrid e-mail addresses and phone numbers for the purposes of notifications of a Data Security Incident.
[12] Include contact details.

# AVANGRID Privacy and Data Security Rider

obligations under any applicable privacy or security law, including but not limited to maintaining Personal Data and Company Data secured, responding to Data Security Incidents, and, where applicable, ensuring the rights of data subjects and carrying out Personal Data impact assessments;

(viii) Inform the CUSTOMER, if, where applicable, data subjects exercise their rights of access, rectification, erasure or objection, restriction of processing, data portability and not to be the subject to automated decisions by the VENDOR. The communication must be made immediately and in no case later than one (1) business day following the receipt of the request by VENDOR. VENDOR shall assist CUSTOMER, taking into account the nature of the Personal Data Processing, through appropriate Technical and Organizational Measures, and with any information that may be relevant to the resolution of the request;

(ix) Not use independent contractors or provide Personal Data or Company Data to independent contractors or other personnel that are not full-time employees of VENDOR without CUSTOMER's prior written approval;

(x) Not disclose Personal Data or Company Data to any third party (including, without limitation, VENDOR's subsidiaries and affiliates and any person or entity acting on behalf of VENDOR) unless with respect to each such disclosure: (A) the disclosure is necessary in order to carry out VENDOR's obligations under the Agreement and this Rider; (B) VENDOR executes a written agreement with such third party whereby such third party expressly assumes the same obligations set forth in this Rider; (C) VENDOR has received CUSTOMER's prior written consent; (D) the Processing is carried out in accordance with the instructions of CUSTOMER, and (D) VENDOR shall remain responsible for any breach of the obligations set forth in this Rider to the same extent as if VENDOR caused such breach;

(xi) Not permit any officer, director, employee, agent, other representative, subsidiary, affiliate, independent contractor, or any other person or entity acting on behalf of VENDOR to Process Personal Data or Company Data unless such Processing is in compliance with this Rider and is necessary to carry out VENDOR's obligations under the Agreement and this Rider. Personal Data and Company Data shall only be accessed by persons who need access to carry out VENDOR's obligations under the Agreement and this Rider and in accordance with the instructions of CUSTOMER; VENDOR shall provide appropriate privacy and security training to its employees and those persons authorized to Process Personal Data or Company Data.

(xii) Establish policies and procedures to provide all reasonable and prompt assistance to CUSTOMER in responding to any and all requests, complaints, or other communications received from any individual who is or may be the subject of any Personal Data Processed by VENDOR to the extent such request, complaint or other communication relates to VENDOR's Processing of such Personal Data;

(xiii) Establish policies and procedures to provide all reasonable and prompt assistance to CUSTOMER 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 Personal Data or Company Data, exfiltration of Personal Data or Company Data, disclosure of Personal Data or Company Data, or misuse of Personal Data or Company Data to the extent such

# AVANGRID Privacy and Data Security Rider

request, complaint or other communication relates to VENDOR's Processing of such Personal Data or Company Data;

(xiv) Not transfer any Personal Data or Company Data across a country border, unless directed to do so in writing by CUSTOMER, and VENDOR agrees that CUSTOMER is solely responsible for determining that any transfer of Personal Data or Company Data across a country border complies with the applicable laws and this Rider;

(xv) Keep Personal Data and Company Data in strict confidence;

(g) At the time of the execution of this Rider, and at any time, upon CUSTOMER's request, VENDOR shall provide evidence that it has established and maintains Technical and Organizational Measures governing the Processing of Personal Data and Company Data appropriate to the Processing and to the nature of the Personal Data and Company Data;

(h) To the extent VENDOR maintains Personal Data and Company Data at its location, CUSTOMER shall have the right to conduct onsite inspections and/or audits (with no advance notice to VENDOR) of VENDOR's information security protocols, and VENDOR agrees to cooperate with CUSTOMER regarding such inspections or audits; provided, any such inspections or audits shall be conducted during normal business hours and in a manner so as to minimize any disruptions to VENDOR's operations. VENDOR will promptly correct any deficiencies in the Technical and Organizational Measures identified by CUSTOMER to VENDOR;

(i) VENDOR shall keep and make accessible to CUSTOMER, at any time, upon CUSTOMER's request, documentation that evidences compliance with the terms of this Rider. CUSTOMER may conduct audits and inspections, either directly or through a third party, and VENDOR agrees to cooperate with CUSTOMER regarding such audits;

(j) VENDOR shall cease Processing Personal Data and Company Data and [return, or securely delete or destroy],[13] or cause or arrange for the [return, or secure deletion or destruction] of, all Personal Data and Company Data subject to the Agreement and this Rider, including all originals and copies of such Personal Data and Company Data in any medium and any materials derived from or incorporating such Personal Data and Company Data, upon the expiration or earlier termination of the Agreement, or when there is no longer any legitimate business need (as determined by CUSTOMER) to retain such Personal Data and Company Data, or otherwise on the instruction of CUSTOMER, but in no event later than ten (10) days from the date of such expiration, earlier termination, expiration of the legitimate business need, or instruction. If applicable law prevents or precludes the return or destruction of any Personal Data or Company Data, VENDOR shall notify CUSTOMER of such reason for not returning or destroying such Personal Data and Company Data and shall not Process such Personal Data and

[13] Personal Data and Company Data in the VENDOR's possession has to be returned or destroyed upon termination or expiration of the agreement or in any of the other scenarios contemplated herein. The business should determine in each case whether the VENDOR will be required to either return the information or destroy the information if what they have are copies.



Take care of the environment.
Printed in black and white and only if necessary.

# AVANGRID Privacy and Data Security Rider

Company Data thereafter without CUSTOMER's express prior written consent. VENDOR's obligations under this Rider to protect the security of Personal Data and Company Data shall survive termination of the Agreement.

(k) [To the extent that VENDOR is afforded regular access in any way to "Cardholder Data" as defined below and for so long as it has such access, the following requirements shall apply with respect to the Cardholder Data; provided, that the parties do anticipate that VENDOR will have access to any Cardholder Data:

(i) VENDOR represents that it is presently in compliance and will remain in compliance with the Payment Card Industry Data Security Standard ("PCI Standard"), and all updates to PCI Standard, developed and published jointly by American Express, Discover, MasterCard and Visa ("Payment Card Brands") for protecting individual credit and debit card account numbers ("Cardholder Data").

(ii) VENDOR acknowledges that Cardholder Data is owned exclusively by CUSTOMER, credit card issuers, the relevant Payment Card Brand, and entities licensed to process credit and debit card transactions on behalf of CUSTOMER, and further acknowledges that such Cardholder Data may be used solely to assist the foregoing parties in completing a transaction, supporting a loyalty program, providing fraud control services, or for other uses specifically required by law, the operating regulations of the Payment Card Brands, or this Agreement.

(iii) To the extent Cardholder Data is regularly maintained on the premises or property of VENDOR, VENDOR shall maintain a business continuity plan addressing the possibility of a potential disruption of service, disaster, failure or interruption of its ordinary business process, which business continuity plan provides for appropriate back-up facilities to ensure VENDOR can continue to fulfill its obligations under the Agreement.

(iv) VENDOR agrees that, in the event of a Data Security Incident arising out of or relating to VENDOR's premises or equipment contained thereon, VENDOR shall afford full cooperation and access to VENDOR's premises, books, logs and records by a designee of the Payment Card Brands to the extent necessary to perform a thorough security review and to validate VENDOR's compliance with the PCI Standards; provided, that such access that be provided during regular business hours and in such a manner so as to minimize the disruption of VENDOR's operations.][14]

(l) [To the extent that the VENDOR processes personal information of California residents as such terms are defined in the California Consumer Privacy Act of 2018, as amended (Cal. Civ. Code §§ 1798.100 to 1798.199.95), the terms and conditions set forth in Schedule D of this Rider shall apply.][15]

[14] This section only has to be included if the VENDOR will be afforded access to Cardholder Data. If the VENDOR will not have access to Cardholder Data, this section can be deleted prior to providing the Rider to the counterparty for review.

[15] Only for Avangrid wide or Avangrid Renewables related engagements where the VENDOR will process personal information of California residents. Not applicable to Avangrid Networks only engagements.

# AVANGRID Privacy and Data Security Rider

(m) [To the extent that VENDOR processes personal data of Connecticut consumers as such terms are defined in An Act Concerning Personal Data Privacy and Online Monitoring (Public Act No. 22-15), the terms and conditions of Schedule E shall apply.][16]

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

(o) In addition to any other insurance required to be provided by VENDOR hereunder, VENDOR shall also provide the Cyber-Insurance coverage meeting the requirements specified in Schedule B, attached hereto and made part hereof. VENDOR shall also comply with the terms and conditions in Schedule B as they relate to any insurance required to be provided by VENDOR pursuant to this Agreement.

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

(q) Failure by VENDOR to comply with any requirement of this Rider shall constitute a material breach of the Agreement and a VENDOR default thereunder. CUSTOMER shall be allowed to terminate the Agreement, and CUSTOMER shall have all rights and remedies provided by law or equity under the Agreement and this Rider.

***

[*Signature page follows*]

[16] Only for agreements that involve (i) The United Illuminating Company, Connecticut Natural Gas, Southern Connecticut Gas or UIL Holdings Corporation, or (ii) Avangrid Service Company or Avangrid Management Company if services will be provided to the companies listed in (i).

# AVANGRID Privacy and Data Security Rider

IN WITNESS WHEREOF, CUSTOMER and VENDOR have caused their representatives to execute and deliver this Privacy and Data Security Rider.

| CUSTOMER | VENDOR |
|---|---|
| By: _____ | By: _____ |
| Name: | Name: |
| Title: | Title: |
| Date: | Date: |
| By: _____ | |
| Name: | |
| Title: | |
| Date: | |

[*Signature page to Privacy and Data Security Rider*]

# AVANGRID Privacy and Data Security Rider

Schedule A

## General Security Requirements

(a) The following definitions are relevant to this General Security Requirements Schedule:

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

(ii) "Protected Information" means Personal Data and Company Data as defined in the Rider.

(iii) Capitalized terms not otherwise defined in this Schedule shall have the meaning set forth in the Rider.

(b) VENDOR must, always, know the level of information protection that should be afforded to the Protected Information as well as the corresponding standards and applicable laws and regulations, and it shall adopt the Technical and Organizational Measures adequate thereto. VENDOR shall, at least, maintain Technical and Organizational Measures consistent with the type of Protected Information being processed and the services being provided by VENDOR, to secure Protected Information, which measures shall implement industry accepted protections which include physical, electronic and procedural safeguards to protect the Protected Information supplied to VENDOR against any Data Security Incident or other security incident, and any security requirements, obligations, specifications or event reporting procedures set forth in the Agreement, the Rider or this Schedule. As part of such security measures, VENDOR shall provide a secure environment for all Protected Information and any hardware and software (including servers, network, and data components) to be provided or used by VENDOR as part of its performance under the Agreement on which Protected Information is contained.

(c) When the scope of the Agreement implies the use or connection of VENDOR's Cyber-infrastructure to that of CUSTOMER, the VENDOR shall have reasonable Technical and Organizational Measures for its protection and for the prevention of any Data Security Incident.

(i) The connection between the CUSTOMER's and the VENDOR's network is not permitted, unless expressly agreed to in writing, in which case it must be done by establishing encrypted and authenticated virtual private networks, and the number of interconnection points between the two

# AVANGRID Privacy and Data Security Rider

networks must be the minimum that is compatible with the required level of availability. The connection to the VENDOR's network shall be removed as soon as there is no need for it.

(ii) Direct user connections from the VENDOR to CUSTOMER's network are not permitted, unless authorized in writing by CUSTOMER and only for a limited period of time.

(iii) If the Agreement is fully or partially performed at the VENDOR's premises or property, the VENDOR must establish mechanisms and procedures for physical access to said premises or property to prevent unauthorised persons from accessing Cyber-infrastructure or Protected Information.

(d) VENDOR shall establish mechanisms and procedures for identifying, authenticating and controlling logical access necessary to prevent unauthorised persons from accessing its Cyber-infrastructure elements and CUSTOMER's Protected Information, and, in particular:

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

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

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

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

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

(ii) The same security measures shall apply to backups as to the original Protected Information.

(f) In the event that CUSTOMER has expressly authorized VENDOR to use its own IT equipment for accessing CUSTOMER's Cyber-infrastructure, the VENDOR shall guarantee and undertake

# AVANGRID Privacy and Data Security Rider

that there are adequate security measures to protect the stationary or portable IT equipment and mobile devices used to access such Cyber-infrastructure or for storing, processing or transmitting the Protected Information, including but not limited to:

(i) Automatic locking if the device is left unattended for a certain period of time. User authentication will be required for unlocking.

(ii) Protection against malicious software and known vulnerabilities.

(iii) Updating the operating system as often as the vendor requires.

The VENDOR shall maintain an action procedure should the equipment or device be lost or stolen, ensuring, to the maximum extent possible that the event be communicated promptly, Protected Information be deleted safely in accordance with recognised standards, and access to CUSTOMER's systems or systems containing CUSTOMER's Protected Information be suspended.

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

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

AVANGRID may request information concerning any Processing of Protected Information by the VENDOR.

(h) The VENDOR shall include security measures appropriate to the nature of the Protected Information Processed in developing, maintaining and testing the equipment that will be used to perform the services being provided by VENDOR. The VENDOR will adopt secure code development standards and ensure that no real data is used in test environments. If necessary, CUSTOMER's express written authorisation will be required, and the same security measures required for the work environment will be applied to these test environments.

(i) When the scope of the Agreement includes the supply of equipment and/or materials, the VENDOR shall prove that best security practices and standards have been applied for the design, fabrication, maintenance, and, where applicable, installation of the supplied equipment and/or materials, including its components.

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



Take care of the environment.
Printed in black and white and only if necessary.

# AVANGRID Privacy and Data Security Rider

(i) The VENDOR shall provide evidence or certificates that guarantee design security, firmware/software updates and malware protection.

(ii) The VENDOR shall conduct periodic analyses of vulnerabilities and inform CUSTOMER about any necessary updates, especially those that affect security.

(iii) All internet connected devices shall be protected with adequately complex passwords that can be changed by CUSTOMER.

(iv) The configuration of devices, equipment and materials shall be adjustable exclusively according to AVANGRID's needs, and any unnecessary functionality deactivated. Should the VENDOR conduct any configuration, documentation to that effect shall be provided.

(j) VENDOR should fully implement the mitigation actions available on the APTs Targeting IT Service Provider CUSTOMERS site page to protect against this malicious activity. VENDOR should implement the following specific actions:

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

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

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

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

# AVANGRID Privacy and Data Security Rider

Schedule B

## Cyber-Insurance Requirements

(a) VENDOR shall during the term of the Agreement have and maintain the following insurance coverage:

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

1) violations of data privacy or data security laws and regulations; and

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

3) other risks specific to the work performed by VENDOR as shall be identified by CUSTOMER.

(ii) Such coverage shall be furnished by an insurance company with an A.M. Best Financial Strength Rating of A- or better, and which is otherwise reasonably acceptable to CUSTOMER.

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

(c) All insurance coverage(s) provided by VENDOR pursuant to this Agreement shall be primary and non-contributing with respect to any other insurance or self-insurance which may be maintained by the CUSTOMER.



Take care of the environment.
Printed in black and white and only if necessary.

# AVANGRID Privacy and Data Security Rider

[Schedule C][17]

## Acceptable Use Requirements

The intent of this Schedule is to document requirements as they pertain to the Acceptable Use of the Electronic Devices and Cyber-infrastructure of Avangrid, Inc. and any of its subsidiaries (hereinafter "Avangrid") by contractors, consultants or other third parties.

Employees and other persons acting on behalf of Avangrid vendors shall be required to read, acknowledge their understanding of, and commit to comply with these Avangrid Acceptable Use Requirements.

## Definitions

- A **User** is defined as any contractor, consultant or other third parties, including any employee of an Avangrid vendor, with access to or using Avangrid Electronic Devices or Cyber-infrastructure.

- **Cyber-infrastructure** Includes electronic information and communications systems and services, and the information contained in these systems and services. Those systems and services are composed of all hardware and software that process (creation, access, modification, and destruction), store (paper, magnetic, electronic, and all other media types), and communicate (sharing and distribution) information, or any combination of these elements.

- **Electronic Devices** include standard computer (workstation desktop/ laptop) with network connections, digital storage media used in standard computers (e.g. hard drives), telephone and voicemail systems, mobile phones, smartphones, tablets, Personal Digital Assistants (PDA), End Point Storage Devices (EPSD), digital and video cameras (including CCTV), mobile navigation systems, printers, photocopiers and scanners, fax machines, and all other similar of associated devices, etc.

    - **Avangrid Electronic Devices** are Electronic Devices owned and managed by Avangrid.

    - **Personally Owned Devices (POD)** are Electronic Devices (e.g. smart phones, tablets, laptops) privately owned and managed by Users.

    - **End Point Storage Devices (EPSD)** applies to the storage of data on devices that can be connected either by a USB drive, data cable or by wireless connection direct to any computing equipment within Avangrid, e.g. USB sticks, drives, thumb nails, pen drives, flash drives, memory cards, etc.

[17] Schedule C (Acceptable Use Requirements) only needs to be included if the VENDOR will have access to Avangrid information technology resources or if the VENDOR will have access to the Avangrid information technology environment.

# AVANGRID Privacy and Data Security Rider

## 1. Requirements and Practices

### 1.1 Electronic Devices

Avangrid Electronic Devices and resources are property of Avangrid and may be provided to Users for the pursuit of their professional activity.

1.1.1 The determining authority and responsibility for issuance of an Electronic Device shall rest with the Avangrid Business Area Leader (BAL) or department hiring manager.

1.1.2 Avangrid Electronic Devices shall be provided to Users configured with the required security hardware and software protections.

a. Compromising or interfering with the Electronic Devices' operating system, hardware, software or protection mechanisms is prohibited.

1.1.3 Users shall be responsible for the appropriate use of authorized Electronic Devices in accordance with their duties and responsibilities, including, but not limited to:

a. Protecting Electronic Devices from misuse.

b. Logging off or protecting Electronic Devices with a screen and/or keyboard locking mechanism, when unattended and when not in use.

i. Desktop and laptop computers shall be switched off or hibernating when unattended for a period more than one hour and always at the end of the workday.

ii. Desktop and laptop computer screens shall be locked by Users always when unattended.

c. Taking the following preventative measures to ensure that any Electronic Devices used to connect to Avangrid's Cyber-infrastructure are physically secured by:

i. Protecting Avangrid assets from unauthorized access and use by others,

ii. Leaving Electronic Devices in secured locations (e.g. locked cabinet or drawer, locked rooms in locked buildings as applicable),

iii. Not leaving Electronic Devices in plain view in unattended vehicles,

iv. Not leaving Electronic Devices in vehicles overnight,

v. Carrying laptops as hand luggage when traveling,



Take care of the environment.
Printed in black and white and only if necessary.

# AVANGRID Privacy and Data Security Rider

vi. Positioning Electronic Devices so that they (and the information displayed) are not visible from outside a ground floor window, and

vii. Positioning the display screen of Electronic Devices such that it cannot be viewed by others in public places (e.g. train, aircraft, restaurants, etc.).

1.1.4 Users shall follow Avangrid procedures for immediately reporting lost, compromised, or stolen Electronic Devices.

a. The User shall notify the Service (Help) Desk and their Avangrid contact.

1.1.5 User shall follow Avangrid procedures for the return of Avangrid owned Electronic Devices when the use of those devices is deemed no longer necessary.

a. Users shall return all Avangrid Electronic Devices to their Avangrid contact immediately upon separation/ termination, which shall be responsible for collecting all Avangrid Electronic Devices.

1.1.6 The use of hot desks/ shared network access equipment shall be reserved for Users who do not regularly require the use of a portable Electronic Device (e.g. laptop) for their professional activities.

a. Users of hot desks/shared network access shall have a current network login.

## 1.2 Connection to Avangrid Cyber-infrastructure

1.2.1 All Electronic Devices which connect to the Avangrid Cyber-infrastructure network shall be Avangrid approved assets which have been configured in accordance with Avangrid standard configurations.

a. Non-Avangrid approved Electronic Devices shall not connect directly to the Avangrid Cyber-infrastructure (e.g. through Ethernet connection).

b. Wireless connections from an Avangrid office shall only be accomplished through Avangrid Electronic Devices and the Avangrid supported wireless infrastructure.

c. Guest wireless network accounts shall only be supplied on ‘as-need-be-basis’ following Avangrid approval processes.

d. Remote desk connections shall only be supplied on ‘as-need-be-basis’ following Avangrid approval processes.

# AVANGRID Privacy and Data Security Rider

## 1.3 Use of Mobile Devices (for Remote Access)

1.3.1 The determining authority and responsibility for issuance of a mobile electronic device to perform Avangrid professional activities; access the Avangrid Cyber-infrastructure or store/transmit Avangrid information/data remotely shall rest with the Avangrid Business Area Leader (BAL) or department hiring manager.

a. Users shall remotely access Avangrid's Cyber-infrastructure utilizing only authorized hardware, software and access control standards (e.g. Avangrid approved VPN technology for Avangrid Electronic Devices or Citrix client).

b. At no time shall a remote User initiate two simultaneous connections to different networks (e.g., no split tunneling and no multi-homed connection).

c. Avangrid issued SIM cards shall not be swapped or used in non-Avangrid issued Electronic Devices.

d. Configuring a non-Avangrid issued Electronic Device for connection to the Avangrid corporate email system is strictly prohibited.

e. Users should be aware that Avangrid may monitor emails sent from and to non-Avangrid issued devices.

## 1.4 Personally Owned Devices

1.4.1 The use of Personally Owned Devices for access to and/or handling of Avangrid information/data and Avangrid Cyber-infrastructure is prohibited.

## 1.5 Treatment of Software and Applications

1.5.1 The acquisition and installation of software on Avangrid Electronic Devices shall be made using approved methods.

a. All access to company software and/or applications shall be subject to formal request and approval processes.

1.5.2 Users shall be prohibited from introducing or installing any unauthorized software, content or material.

1.5.3 The installation of any type of network access program peer (P2P) or similar (e.g., BitTorrent, Emule), as well as any other application for file sharing that could saturate Internet bandwidth, prevent access to other Users or slow down connections to technology and information resources is prohibited.



Take care of the environment.
Printed in black and white and only if necessary.

# AVANGRID Privacy and Data Security Rider

1.5.4 Intellectual property, licensing and regulatory requirements shall be observed always. Downloading, obtaining, copying or redistributing materials protected by copyright, trademark, trade secret or other intellectual property rights (including software, music, video, images) is prohibited, even where such material is to be used for the pursuit of the professional activity.

a. Where materials protected by copyright, trademark, trade secret or other intellectual property rights are required for the pursuit of an Avangrid professional activity the appropriate license/permission shall be obtained prior to use.

## 1.6 Treatment of Information/Data

1.6.1 Information/data assets obtained or created during the engagement with Avangrid are the property of Avangrid and shall be treated in accordance with the applicable Agreement and Data Security Rider.

1.6.2 The storage of Avangrid information/data on Personally Owned Devices or non-Avangrid controlled or authorized environments, including non-authorized Electronic Devices is prohibited. Users shall not store AVANGRID owned information/data on devices that are not issued by AVANGRID unless explicitly and contractually agreed by both parties.

1.6.3 Where access to Personal Data is part of a Users' professional role and responsibilities, access shall be treated in accordance with all applicable data protection and/or privacy law(s) and regulation(s) and under strict access and usage guidelines.

1.6.4 Corporate storage spaces and network resources shall be used for file storage and/or exchange of professional information.

1.6.5 Users shall store and share information/data in accordance with the terms and conditions with Avangrid and any applicable Data Security Rider.

1.6.6 Use of an End Point Storage Device (EPSD) (e.g., USB) shall be limited to those devices acquired through the Information Technology (IT) request process (e.g. ITSM/ServiceNow).

1.6.7 Printed information/data (hard copy) shall be:

a. Stored based on critically, e.g., hardcopy containing confidential and/or sensitive information/data shall be locked away when not required (or not in use).

b. Discarded, when no longer needed, based on criticality, e.g. confidential and/or sensitive hardcopy shall be shredded.

c. To be removed from printers, fax machines, copier rooms, and conference/ meeting rooms immediately.

# AVANGRID Privacy and Data Security Rider

## 1.7 User Access Credentials and Passwords

1.7.1 Requests for access shall be made following access provisioning procedures.

1.7.2 Applications and network resources access shall be activated\deactivated in accordance with Avangrid activation\ deactivation procedures.

1.7.3 Users requiring duly justified privileged access rights will be assigned a specific “Privileged User ID”

a. Privileged User IDs shall be reviewed and confirmed at least semi-annually.

b. Regular professional activities shall not be performed from a privileged ID.

1.7.4 Users shall use strong, complex passwords and securely maintain secret authentication information (e.g. passwords, cryptographic keys, smart cards that produce authorization codes), including:

a. Not sharing or disclosing their Avangrid credentials (log on IDs-user names and/or passwords) with others inside or outside the company.

b. Keeping secret authentication information confidential, ensuring that it is not divulged to any other parties, including senior management and technical support.

c. Not recording (e.g. on paper, software file or hand-held device) secret authentication information, unless this can be stored securely, and the method of storing has been approved (e.g. password vault) by Corporate Security.

d. Changing secret authentication information when there is any indication of a possible compromise.

e. Reporting any incidents or suspected compromises by following Avangrid incident reporting procedures.

## 1.8 Internet Use and Social Media

1.8.1 Avangrid may make available internet access to users depending on their role and responsibilities.

a. Internet access shall be provided as a tool for business purposes, shall be used with moderation and shall be proportional to the work being undertaken.

b. Access to restricted websites shall be enabled at the discretion of Avangrid and shall be

# AVANGRID Privacy and Data Security Rider

provisioned following the security exception process.

c. Only Avangrid approved surfing software shall be used to access the Internet.

1.8.2 A moderate and proportional use of the internet shall be allowed for non-professional activities, although web surfing is expressly prohibited for:

a. Accessing or posting of any racist or sexual content or any material that is offensive or defamatory in nature.

b. Accessing games, downloading video, music (MP3 or another format), or downloading any other files not related to the Avangrid related responsibilities.

1.8.3 Limited and occasional use of Avangrid Electronic Devices and resources to engage in Social Networking[18] and Blogging[19] is acceptable, provided that:

a. It is done in a professional and responsible manner.

b. It does not violate the Code of Ethics or any relevant Avangrid policy, procedure or rule.

c. It is not detrimental to Avangrid's best interests.

d. It does not interfere with regular work duties.

e. There is no breach of the prohibitions identified in these requirements.

1.8.4 Avangrid reserves the right to determine which websites and social media platforms can be accessible through Avangrid Electronic Devices or Cyber –infrastructure.

## 1.9 E-mail Use

1.9.1 All information created, sent, or received via Avangrid's e-mail system(s), including all e-mail messages and electronic files shall be the property of Avangrid.

1.9.2 Avangrid reserves the right to monitor, inspect and access such emails and electronic files.

1.9.3 The forwarding of Avangrid owned information/data to a personal e-mail account is prohibited.

[18] Social Networking is the use of dedicated websites and applications to interact with other users or to find people with similar interests.
[19] Blogging: A blog is a website containing a writer's or group of writers' own experiences, observations, opinions, etc., Blogging is posting to that website.



Take care of the environment.
Printed in black and white and only if necessary.

# AVANGRID Privacy and Data Security Rider

1.9.4 Removing or circumventing any of the security controls enforced on the company email system (e.g. SPAM filtering, automatic email disclaimers, etc.) is prohibited.

1.9.5 Users shall not permit others to use their e-mail accounts. Based on user established permissions; calendars and/or mailboxes may be shared.

1.9.6 Limited use of an Avangrid e-mail account for personal purposes shall be regarded as acceptable provided that:

a. Use does not interfere with the normal performance of professional duties.

b. Messaging does not violate applicable laws, regulations, the Code of Ethics, or Avangrid policies.

c. Use is moderate both in terms of frequency and amount of memory and resources consumed.

1.9.7 Avangrid e-mails or messages containing company information/ data shall not be forwarded to external parties except where there is a specific business 'need to know'.

1.9.8 Avangrid electronic messaging shall not be used for transmitting, retrieving or storing any messages, files or attachments which constitute:

a. Harassing or discriminatory messages which relate to gender, race, sexual orientation, religion, disability or other characteristics protected by applicable laws and regulations.

b. Defamatory messages which adversely affect the reputation of a person or company.

c. Messages that violate copyright, trademark, trade secret or other intellectual property rights.

d. Obscene materials or images of a sexual nature.

e. Files or documents of an indeterminate origin or that, for any reason, may include computer viruses or in any way breach the security systems of the company or the recipient of the file or document, or may damage their IT systems.

f. Any material or images that might reasonably be expected to cause personal offense to the recipient.

g. Messages in violation of applicable laws, regulations, the Code of Ethics, or Avangrid policies.

1.9.9 The retention period for e-mail messages shall be 18 months. Once the retention period has been reached, emails shall be automatically eliminated from the user's mailbox.

# AVANGRID Privacy and Data Security Rider

a. a. Users shall store messages and/or associated attachments in Avangrid provided network folders. Storage of messages and/or associated attachments on hard drives in .pst (personal mail folders) folders is prohibited.

1.9.10 Users shall report suspicious email messages (e.g., spam, phishing, etc.) the Service (Help) Desk and/or using the reporting tool REPORTER, available in Outlook.

## 1.10 Incident reporting

1.10.1 Users shall immediately report any unusual activity, incident or suspected event following Avangrid incident reporting procedures (e.g., Service (Help) Desk, REPORTER, etc.)

## 1.11 Contract Termination

1.11.1 Avangrid Electronic Devices assigned to or in the possession of a User shall be returned to Avangrid on or before the contract termination date or whenever it is determined that the use of the Electronic Device is no longer necessary. This includes the return of facility access badges.

1.11.2 Access to Cyber-infrastructure shall be deactivated (revoked) on or before a User's termination date in accordance with Avangrid access management processes.

## 2. No Expectation of Privacy

All contents of the Avangrid Electronic Devices and Cyber-infrastructure are the property of the company. Therefore, Users should have no expectation of privacy whatsoever in any e-mail message, file, data, document, facsimile, telephone conversation, social media post, conversation, or any other kind or form of information or communication transmitted to, received, or printed from, or stored or recorded on Avangrid's Electronic Devices or Cyber-Infrastructure.

## 3. Monitoring

3.1 Avangrid reserves the right to use monitoring controls, including software, to ensure compliance with these Acceptable Use Requirements document, and to record and/or monitor one or more Users' Electronic Devices and resources, e-mails and/or internet activity in accordance with regulatory and legal requirements.

a. This includes the right to monitor, intercept, access, record, disclose, inspect, review, retrieve, print, recover or duplicate, directly or through third parties designated for such purpose, any information/data contained on and any uses of the Electronic Devices and Cyber-Infrastructure. Avangrid may store copies of such information/data for a period of time after they are created and may delete such copies from time to time without notice. Users consent to such monitoring by acknowledging these requirements and using the Electronic Devices and Cyber-Infrastructure.



Take care of the environment.
Printed in black and white and only if necessary.

# AVANGRID Privacy and Data Security Rider

b. Accordingly, Users should not harbor any expectation of privacy in respect to the use of Avangrid Electronic Devices or Cyber-Infrastructure and should not consider the data contained on them as private.

4.2 Monitoring may take place at any time and without the need to notify or inform the User in advance, taking into consideration legal or regulatory limitations, where applicable.

## 4. Non Compliance

Violation and non-conformance to this guidance by third party workers may result in appropriate actions, including contract termination.

# AVANGRID Privacy and Data Security Rider

[Schedule D][20]

## CCPA Contract Clauses for Service Providers

1. Definitions. The following definitions and rules of interpretation apply in this Schedule:
    a. "Agreement" has the meaning set forth in the Rider.
    b. "CCPA" means the California Consumer Privacy Act of 2018, as amended, including by the California Privacy Rights Act of 2020 (2020 Cal. Legis. Serv. Proposition 24) (Cal. Civ. Code §§ 1798.100 to 1798.199.95), the CCPA Regulations (Cal. Code Regs. tit. 11, §§ 7000 to 7102), and any related regulations or guidance provided by the California Attorney General. Terms defined in the CCPA, including personal information and business purposes, carry the same meaning in this Schedule.
    c. "Contracted Business Purposes" means the services described in the Agreement or the Rider for which the service provider receives or accesses personal information.
    d. "CUSTOMER" has the meaning set forth in the Rider.
    e. "Rider" means the Privacy and Data Security Rider to which this Schedule is appended.
    f. "VENDOR" has the meaning set forth in the Rider.
2. Scope of Application

This Schedule applies only where, and to the extent that, VENDOR processes personal information that is subject to the CCPA on behalf of CUSTOMER in connection with the Agreement.

3. Service Provider's CCPA Obligations
    a. Personal information is disclosed by CUSTOMER to VENDOR only for the specific Contracted Business Purposes. VENDOR will only collect, use, retain, or disclose personal information for the Contracted Business Purposes for which CUSTOMER provides or permits personal information access and in accordance with CUSTOMER's instructions.
    b. VENDOR will not sell or share personal information.
    c. VENDOR will not use, retain or disclose personal information for VENDOR's own commercial purposes or in a way that does not comply with the CCPA. If a law requires the VENDOR to disclose personal information for a purpose unrelated to the Contracted Business Purpose, the VENDOR must first inform the CUSTOMER of the legal requirement and give the CUSTOMER an opportunity to object or challenge the requirement, unless the law prohibits such notice.
    d. VENDOR will not use, retain or disclose personal information outside of the direct business relationship between VENDOR and CUSTOMER.

[20] Schedule D only needs to be included for Avangrid wide or Avangrid Renewables related engagements where the VENDOR will process personal information of California residents.



Take care of the environment.
Printed in black and white and only if necessary.

# AVANGRID Privacy and Data Security Rider

e. VENDOR will not combine personal information that it receives from, or on behalf of, CUSTOMER with personal information it receives from, or on behalf of, another person or persons, or collects from its own interactions with the consumer.
f. VENDOR will limit personal information collection, use, retention, and disclosure to activities reasonably necessary and proportionate to achieve the Contracted Business Purposes.
g. VENDOR must promptly comply with any CUSTOMER request or instruction requiring the VENDOR to provide, amend, transfer, or delete the personal information, or to stop, mitigate, or remedy any unauthorized processing, including any unauthorized use, of personal information.
h. If the Contracted Business Purposes require the collection of personal information from individuals on the CUSTOMER's behalf, VENDOR will always provide a CCPA-compliant notice at collection that the CUSTOMER specifically pre-approves in writing. VENDOR will not modify or alter the notice in any way without the CUSTOMER's prior written consent.
i. If VENDOR determines that it can no longer meet its obligations under the CCPA, VENDOR must promptly notify CUSTOMER.

4. Assistance with Customer's CCPA Obligations
    1. VENDOR will reasonably cooperate and assist CUSTOMER with meeting the CUSTOMER's CCPA compliance obligations and responding to CCPA-related inquiries, including responding to verifiable consumer requests, taking into account the nature of VENDOR's processing and the information available to VENDOR.
    2. VENDOR must notify CUSTOMER immediately if it receives any complaint, notice, or communication that directly or indirectly relates either party's compliance with the CCPA. Specifically, VENDOR must notify the CUSTOMER within 2 working days if it receives a verifiable consumer request under the CCPA.
5. Subcontracting
    a. If CUSTOMER authorizes VENDOR to engage subcontractors in accordance with the terms of the Agreement and the Rider, any subcontractor used must qualify as a service provider under the CCPA and VENDOR cannot make any disclosures to the subcontractor that the CCPA would treat as a sale or share.
    b. For each subcontractor used, VENDOR will:
        i. Promptly notify CUSTOMER of the engagement.
        ii. Engage the subcontractor pursuant to a written contract binding the subcontractor to observe all the requirements set forth in the Rider and this Schedule.
        iii. Provide CUSTOMER with the following information: the subcontractor's name, address, and contact information, the type of services to be provided by the subcontractor, and the personal information categories to be disclosed to the subcontractor.

# AVANGRID Privacy and Data Security Rider

a. VENDOR remains fully liable to the CUSTOMER for the subcontractor's performance of its agreement obligations.
b. Upon the CUSTOMER written request, VENDOR will audit a subcontractor's compliance with its personal information obligations and provide the CUSTOMER with the audit results.

6. CCPA Warranties and Certification
   a. When collecting, using, retaining, disclosing or, in general, processing personal information, VENDOR will comply with all applicable requirements of the CCPA and provide the same level of privacy protection as required by the CCPA.
   b. VENDOR certifies that it understands this Schedule's and the CCPA's restrictions and prohibitions on selling and sharing personal information and retaining, using, or disclosing personal information outside of the parties' direct business relationship, and it will comply with them.

**APPENDIX A**
**Personal Information Processing Purposes and Details**

**Personal Information Categories**: The Agreement involves the following types of personal information, as defined and classified in CCPA

| **Personal Information Category** | **Examples** | **Processed under this Agreement** |
|---|---|---|
| A. Identifiers. | A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers. | [YES/NO] |
| B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)). | A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.<br>Some personal information included in this category may overlap with other categories. | [YES/NO] |
| C. Protected classification characteristics under California or federal law. | Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information). | [YES/NO] |



Take care of the environment.
Printed in black and white and only if necessary.

# AVANGRID Privacy and Data Security Rider

| | | |
|---|---|---|
| D. Commercial information. | Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies. | [YES/NO] |
| E. Biometric information. | Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data. | [YES/NO] |
| F. Internet or other similar network activity. | Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement. | [YES/NO] |
| G. Geolocation data. | Physical location or movements. | [YES/NO] |
| H. Sensory data. | Audio, electronic, visual, thermal, olfactory, or similar information. | [YES/NO] |
| I. Professional or employment-related information. | Current or past job history or performance evaluations. | [YES/NO] |
| J. Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)). | Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records. | [YES/NO] |
| K. Inferences drawn from other personal information. | Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes. | [YES/NO] |

| **Sensitive Personal Information Category** | **Processed under the Agreement** |
|---|---|
| Social security, driver's license, state identification card, or passport number. | [YES/NO] |
| Log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account. | [YES/NO] |

# AVANGRID Privacy and Data Security Rider

| | |
|---|---|
| Precise geolocation. | [YES/NO] |
| Racial or ethnic origin, religious or philosophical beliefs, or union membership. | [YES/NO] |
| Mail, email, or text messages contents not direct to CUSTOMER | [YES/NO] |
| Genetic data. | [YES/NO] |
| Unique identifying biometric information | [YES/NO] |
| Health information | [YES/NO] |



Take care of the environment.
Printed in black and white and only if necessary.

# AVANGRID Privacy and Data Security Rider

[Schedule E][21]

## Connecticut Privacy Act Clauses for Processors

1. Definitions. The following definitions and rules of interpretation apply in this Schedule:
    a. "Agreement" has the meaning set forth in the Rider.
    b. "Connecticut Privacy Act" means Connecticut Act Concerning Personal Data Privacy and Online Monitoring (Public Act No. 22-15). Terms defined in the Connecticut Privacy Act, including personal data and processing, carry the same meaning in this Schedule.
    c. "CUSTOMER" has the meaning set forth in the Rider.
    d. "Rider" means the Privacy and Data Security Rider to which this Schedule is appended.
    e. "VENDOR" has the meaning set forth in the Rider.
2. Scope of Application

This Schedule applies only where, and to the extent that, VENDOR processes personal data that is subject to the Connecticut Privacy Act on behalf of CUSTOMER in connection with the Agreement.

1. Personal data processing by VENDOR
    a. The instructions for the processing of the personal data, the nature and purpose of the processing of the personal data, the type of personal data subject to the processing and the duration for the processing are set forth in section [(d)(ii)][22] of the Rider.
    b. The rights and obligations of CUSTOMER and VENDOR with respect to the processing of personal data are set forth in the Rider and this Schedule.
2. Processor's Connecticut Privacy Act Obligations
    a. VENDOR will ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data.
    b. At CUSTOMER's direction, VENDOR shall delete or return all personal data to the CUSTOMER as requested at the end of the provision of the services, unless retention of data is required by law.
    c. Upon reasonable request from CUSTOMER, VENDOR shall make available to CUSTOMER all information in its possession necessary to demonstrate the processor's compliance with the obligations in sections 1 to 11, inclusive, of the Connecticut Privacy Act.

[21] Only for agreements that involve (i) The United Illuminating Company, Connecticut Natural Gas, Southern Connecticut Gas or UIL Holdings Corporation, or (ii) Avangrid Service Company or Avangrid Management Company if services will be provided to the companies listed in (i).
[22] Confirm cross reference before execution.



Take care of the environment.
Printed in black and white and only if necessary.

# AVANGRID Privacy and Data Security Rider

d. VENDOR shall, allow, and cooperate with, reasonable assessments by CUSTOMER or CUSTOMER's designated assessor, or the VENDOR may, at its own cost, arrange for a qualified and independent assessor to conduct an assessment of the VENDOR's policies and technical and organizational measures in support of the obligations under sections 1 to 11, inclusive, of the Connecticut Privacy Act, using an appropriate and accepted control standard or framework and assessment procedure for such assessments, and provide a report of such assessment to CUSTOMER upon request.

3. Subcontracting
   c. If CUSTOMER authorizes VENDOR to engage subcontractors in accordance with the terms of the Agreement and the Rider, any subcontractor engaged by VENDOR to process personal data shall be engaged pursuant to a written contract that requires the subcontractor to meet the obligations of VENDOR with respect to personal data.
2. Connecticut Privacy Act Warranties
   a. VENDOR will comply with all applicable requirements of the Connecticut Privacy Act when processing personal data.



Take care of the environment.
Printed in black and white and only if necessary.