AVANGRID

May 2017

AVANGRID Data Security Rider

A.1 Privacy and Data Security.

(a) To the extent that [insert name of third party supplier/contractor] (sometimes hereinafter referred to as "VENDOR") is regularly afforded access in any way to "Personal Data" or "Company Data" as defined below, this Rider shall apply with respect to Personal Data and Company Data.

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

(i) "Personal Data" means any information that can be used to identify, locate, or contact an individual, including an employee, customer, or potential customer of CUSTOMER (also sometimes hereinafter referred to as "Company"), including, without limitation: (A) first and last name; (B) home or other physical address; (C) telephone number; (D) email address or online identifier associated with an individual; (E) "Sensitive Data" as defined below; (F) ZIP codes; (G) employment, financial or health information; or (H) any other information relating to an individual, including cookie information and usage and traffic data or profiles, that is combined with any of the foregoing.

(ii) "Sensitive Data" is that subset of Personal Data, including Social Security number, passport number, driver's license number, or similar identifier, or credit or debit card number, whose unauthorized disclosure or use could reasonably entail enhanced potential risk for the data subject.

(iii) "Company Data" means any information that relates to the operation or functionality of plants, factories, networks, or grids of the Company or to which the Company has access, including, without limitation, Critical Infrastructure Information and internal financial information.

(iv) "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 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.

(v) "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, use, disclosure, dissemination, exfiltration, taking, removing, copying, making available, alignment, combination, blocking, deletion, erasure, or destruction.

(vi) "Data Security Breach" 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; or (C) any

other act or omission that compromises the security, confidentiality, or integrity of Personal Data or Company Data.

(vii) "Technical and Organizational Security 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 Breach, and any security requirements, obligations, specifications or event reporting procedures set forth in any Schedule to this Agreement. 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 this Agreement on which Personal Data and Company Data is contained to the extent the same are located on VENDOR's premises.

(viii) "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).

(c) Personal Data and Company Data shall at all times remain the sole property of CUSTOMER, and nothing in this 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 and Company Data.

(d) VENDOR shall 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 before doing so.

(e) VENDOR shall Process Personal Data and Company Data only on the instruction of CUSTOMER and in accordance with this Agreement and privacy and security laws applicable to VENDOR's services or VENDOR's possession or Processing of Personal Data and\or Company. CUSTOMER hereby instructs VENDOR, and VENDOR hereby agrees, to Process Personal Data or Company Data as necessary to perform VENDOR's obligations under this Agreement and for no other purpose.

(f) 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 this Agreement and as authorized by CUSTOMER.

(g) As a condition to starting work, VENDOR's employees shall acknowledge in writing their agreement to comply with the terms of the Company'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 Company.

AVANGRID Data Security Rider

(h) 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, and not, by act or omission, place CUSTOMER in violation of any privacy or security law known by VENDOR to be applicable to CUSTOMER;

(ii) Have in place appropriate and reasonable Technical and Organizational Security Measures to protect the security of Personal Data and Company Data and prevent a Data Security Breach, including, without limitation, a breach 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;

(iii) Safely secure or encrypt all Sensitive Data and Company Data during storage or transmission;

(iv) Except as may be necessary in connection with providing Support Services (and provided that immediately upon the need for such Personal Data and Company Data ceasing, such Personal 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;

(v) Notify CUSTOMER no later than one (1) day from the date of obtaining actual knowledge of any Data Security Breach 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;

(vi) 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 Agreement and is necessary in order to carry out VENDOR's obligations under this Agreement;

(vii) 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 this Agreement; (B) such third party is bound by the same provisions and obligations set forth in this Agreement; (C) VENDOR has received CUSTOMER's prior written consent; and (D) VENDOR shall remain responsible for any breach of the obligations set forth in this Agreement to the same extent as if VENDOR caused such breach; and

(viii) 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 or Company Data Processed by VENDOR to the extent such request, complaint or other communication relates to VENDOR's Processing of such Personal Data.

(ix) 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 request, complaint or other communication relates to VENDOR's Processing of such Personal Data or Company Data.

(x) 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 under this Contract complies with the applicable data protection laws and this Contract.

(i) At the time of the signing of this agreement, and at the time of any CUSTOMER request, VENDOR shall provide evidence that it has established and maintains Technical and Organizational Security Measures governing the Processing of Personal Data and Company Data appropriate to the Processing and the nature of the Personal Data and Company Data to be protected. 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 Security Measures identified by CUSTOMER to VENDOR.

(j) VENDOR shall return, delete, or destroy, or cause or arrange for the return, deletion, or destruction of, all Personal Data and Company Data subject to this Agreement, 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 this 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 Company Data thereafter without CUSTOMER's express prior written consent. VENDOR's obligations under this Agreement to protect the security of Personal Data and Company Data shall survive termination of this Agreement.

AVANGRID Data Security Rider

(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 this Agreement.

(iv) VENDOR agrees that, in the event of a Data Security Breach 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.

(l) To the extent VENDOR is provided regular access to Personal Data, Company Data, or Cardholder Data, VENDOR represents that the security measures it takes in performance of its obligations under this Agreement are, and will at all times remain, at the highest of the following (collectively referred to herein as "Security Best Practices"): (a) Privacy & IT Security Best Practices (as defined by ISO 27001/27002); and (b) any security requirements, obligations, specifications, or event reporting procedures set forth in Schedule A.

(m) 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.

AVANGRID Data Security Rider

(n) Notwithstanding anything in the Agreement to the contrary, VENDOR shall indemnify, defend and hold CUSTOMER harmless from and against all Losses suffered or sustained by the CUSTOMER, its affiliates, and their respective employees, officers, representatives, or contractors, or by any third party or entity, caused by, resulting from, or attributable to VENDOR's breach or violation of any of the terms and conditions of this Data Security Rider. VENDOR's obligation to indemnify defends, and hold CUSTOMER harmless shall survive termination or expiration of the Agreement.

(o) Failure by VENDOR to comply with any requirement of this section shall constitute a material breach of the contract.

***

AVANGRID

May 2017

AVANGRID Data Security Rider

Schedule A

General Security Requirements

[Specific requirements to be developed as needed]

AVANGRID

May 2017

AVANGRID Data Security Rider

Schedule B

Cyber-Insurance Requirements

(a) Vendor shall during the term of this 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) and other risks specific to the work performed by Vendor as shall be identified by Company.

(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.

AVANGRID

May 2017

AVANGRID Data Security Rider

Schedule C

Acceptable Use Requirements – Procedural Guidance

The intent of this procedural guidance is to document requirements as it pertains to the Acceptable Use of AVANGRID's Electronic Resources, Electronic Messaging, and the Internet/Intranet by Third Party Workers.

All Third Party Workers shall be required to read and acknowledge their understanding of the AVANGRID Acceptable Use Requirements.

Definitions

Acceptable Use: For purposes of these requirements document, acceptable use is the corporate organizational rules governing the use of electronic resources, electronic messaging, and Internet/Intranet usage.

Electronic Resources: computing and telecommunications devices that can execute programs or store data; examples of which may include, but are not limited to: computers, mobile computing devices, smartphones, portable wireless network access devices and storage devices (USB or otherwise connected).

Electronic Messaging: includes email, IM, audio-video conferencing and any other one-to-one, one-to-many, or many-to-many personal communications. (AVANGRID e-mail system, network, or Internet/Intranet access).

Third Party Worker: means contract employees, employees of suppliers or contractors, employees of consultants, or any other third party worker.

Questions pertaining to the contents of the AVANGRID Acceptable Use Requirements shall be directed, in writing, to the CSO at: Corporate.SecurityUSA@Avangrid.com. Responses shall be made in writing.

Acceptable Use Policy

AVANGRID Data Security Rider

Requirements

1.0 Electronic Resources

1.1 Third Party Workers shall be responsible for the appropriate use and security of information (data) when using any AVANGRID electronic resource.

a. Appropriate use shall include using authorized AVANGRID electronic resources as intended by AVANGRID in accordance with duties and responsibilities.

i. Using AVANGRID electronic resources in violation of these requirements, or any negligent or unlawful activity shall be considered inappropriate use.

1.2 Within each AVANGRID business area and/or department the determining authority and responsibility for issuance of an electronic resource shall rest with the Business Area Leader, department/ hiring manager and, in some instances, the Information Technology department (ex: laptops).

1.3 Third Party Workers shall be prohibited from introducing any unauthorized electronic resources or software into the AVANGRID environment, including without limitation any electronic resources or software that could disrupt any operations or compromise security.

1.4 Third Party Workers shall not store AVANGRID owned information/data on devices that are not issued by AVANGRID unless explicitly and contractually agreed by both parties.

1.5 AVANGRID electronic resources shall be protected from misuse, including, but not limited to: theft, unauthorized access, fraudulent manipulation and alteration of data, attempts to circumvent security controls, and any activity that could compromise the confidentiality, integrity, or availability of information (data).

1.6 Third Party Workers shall immediately report lost, compromised, or stolen electronic AVANGRID resources to the IT Service Desk and their AVANGRID department manager.

1.7 Any AVANGRID electronic resources assigned to or in the possession of a Third Party Worker shall be returned to a designated individual within his/her AVANGRID department when it is determined by department management that the use of those resources is no longer necessary or upon completion of the engagement for which this device was provided.

1.8 Authorized Third Party Workers may remotely access the AVANGRID IT managed corporate network utilizing only approved hardware, software and access control standards.

a. Remote access requests shall be approved by management and are restricted to computing resources that authorized users require to perform their job responsibilities.

1.9 Third Party Workers shall not share or disclose their AVANGRID credentials (log on ids and/or passwords) with others.

2.0 Electronic Messaging

2.1 Conducting AVANGRID business that results in the storage of AVANGRID owned information/data on personal or non-AVANGRID controlled environments, including devices maintained by a third-party with whom AVANGRID does not have a contractual agreement shall be prohibited.

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

2.3 Third Party Workers shall:

a. Use caution to ensure that the correct e-mail address is used for the intended recipient(s) (e.g., with the use of auto fill, reply all, etc.).
   i. Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any AVANGRID electronic communication to mislead the recipient about the identity of the sender shall be prohibited.

b. Not send spam via e-mail, text messages, pages, instant messages, voice mail or other forms of electronic communication.

c. Posting to a public newsgroup, bulletin board, blog, listserv with an AVANGRID e-mail or IP address is strictly prohibited.
   i. Avoid Representing or appearing to represent the opinions of AVANGRID is prohibited unless appropriately authorized to do so.

2.4 AVANGRID's electronic messaging is intended to support legitimate business requirements. Limited use of AVANGRID electronic messaging facilities for personal purposes shall be regarded as acceptable provided that:

a. Messages are not used for private business or other commercial purposes, including the sale or purchase of goods or services, or engaging with other clients.

b. Use does not interfere with the normal performance of workers' duties,
c. There is no breach of the prohibitions identified in these requirements,
d. Messaging does not violate applicable laws, regulations, the Code of Ethics, or AVANGRID policies.

2.5 AVANGRID's electronic messaging shall not be used for transmitting, retrieving or storing any messages, files or attachments which constitute:

a. Harassing or unwanted messages (including insults and 'jokes'), including offensive messages which relate to gender, race, sexual orientation, religion, disability or other similar subject matter.
b. Defamatory messages which adversely affect the reputation of a person or company.
c. Messages that violate copyright, trademark, or other intellectual property rights of another party.
d. Obscene materials of an offensive or sexual nature.
e. Offensive material that might reasonably be expected to cause distress or other personal offense to the recipient.
f. Messages in violation of applicable laws, regulations, the Code of Ethics, or AVANGRID policies.

2.6 Third Party Workers shall not disclose their passwords to others or permit others to use their e-mail accounts.

2.7 Third Party Workers shall never assume the privacy or confidentiality of electronic messages.

a. This includes information (data) protected by local, national or international
b. security and privacy regulations and standards as well as data protected by confidentiality agreements.

b. Third Party Workers shall restrict transmission of such protected information to the extent feasible and utilize security procedures made available by AVANGRID, and in accordance with contractual agreements.

3.0 Wireless Communications

3.1 All wireless infrastructure devices that reside at AVANGRID sites and connect to an AVANGRID network, or provides access to sensitive or confidential information shall:

a. Be installed, supported and maintained by AVANGRID or its designee

b. Use AVANGRID approved authentication protocols, infrastructure, and encryption protocols
c. Maintain a hardware address that can be registered and tracked

3.2 Under no circumstances are unauthorized wireless communication devices allowed to directly connect to the internal AVANGRID corporate network.

3.3 Internet access through wireless technology (hotspots) not belonging to AVANGRID shall only be used if contractually agreed by AVANGRID and the Third Party Worker.

4.0 BYOD (Bring Your Own Device)

4.1 AVANGRID does not support the use of personally owned devices (POD)1 by Third Party Workers to perform business functions, except:

a. Short term engagements for professional services or consulting services where Third Party Workers will use third party owned equipment in the performance of contractually agreed upon duties, tasks and deliverables.

5.0 End Point Data Storage Devices

5.1 AVANGRID does not recommend the use of third party or user -owned End Point Data Storage Devices (EPSD) due to security risks. In the event that an EPSD is required, the AVANGRID Corporate Security Office shall distribute an approved device upon receipt of an approved ITSM request.

a. It is expected that Third Party Workers engaged in professional services or consulting services shall utilize contractually agreed methods for file storage and sharing as their primary/preferred means for file storage.

b. 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.

6.0 Clear Desk & Screen

[1] PODs are information and communications technology devices (e.g. smart phones, lap tops) owned by employees or by third parties (such as suppliers, consultants and maintenance contractors).

6.1 Third Party Workers shall take steps to ensure a clear desk, screen and workplace by:

a. Locking away business critical and/or sensitive information, e.g. on paper or on electronic storage media, when not required (or not in use), and when the office (or work space) is unoccupied.
b. Shredding business critical and/or sensitive documentation when no longer needed, consistent with the Company's record retention policies.
c. Logging off or protecting computing resources (desktops, laptops, terminals, etc.) with a screen and/or keyboard locking mechanism, controlled by a password, token or similar user authentication mechanism when unattended and when not in use.
d. Using photocopiers and other reproduction technology (e.g. scanners, digital cameras) only as necessary and authorized to do so.
e. Removing materials containing business critical, sensitive or classified information from printers, fax machines, copier rooms, and conference/meeting rooms immediately.

7.0 Monitoring

7.1 AVANGRID reserves the right to use monitoring controls, including software, to ensure compliance with this Acceptable Use Requirements document. AVANGRID may record and/or monitor one or more Third Party Workers' AVANGRID's owned computer and/or internet activity for any reason and without prior notice.

7.2 Under no circumstances is personal or third party computing equipment allowed to directly connect to the internal AVANGRID-IT managed corporate network, either by wired connection or via approved wireless protocol. AVANGRID IT reserves the right to monitor and remove unauthorized connections without prior notice.

8.0 Return of Electronic Resources

8.1 Voluntary Termination

a. Third Party Workers shall return all AVANGRID electronic resources assigned to them or in their possession, to a designated individual, within twenty-four (24) hours of notice of termination or before their documented last day of work. AVANGRID business management shall make that determination. This includes return of facility access badges.

8.2 Involuntary Termination

a. Third Party Workers shall return all electronic resources assigned to them or in their possession immediately upon notice of termination. This includes return of facility access badges.

9.0 Compliance & Reporting

9.1 A violation of the AVANGRID Acceptable Use Requirements by a temporary Third Party Worker, contractor or consultant may result in termination of their contract or assignment with AVANGRID.

9.2 Suspected requirements violations, system intrusions, virus outbreaks and other conditions which might jeopardize AVANGRID's information or computing resources shall be immediately reported to the IT Service Desk.