This Privacy and Data Security Rider (the “Rider”) is entered by [insert name of third party supplier/contractor] (“VENDOR”) and [insert the name of the contracting Avangrid entity]. For the purposes of this Rider [insert the name of the contracting Avangrid entity] and any of its affiliates procuring or receiving services, works, equipment or materials under the Agreement shall be hereinafter referred to as the “CUSTOMER”.

1. 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 execution of the Agreement, and establish the obligations and responsibilities of the VENDOR derived from such Processing.
2. The following definitions are relevant to this Rider:
	1. “Personal Data” means any information about an individual, including an employee, 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) “Sensitive Personal Data” as defined below; 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.
	2. “Sensitive Personal 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 individual.
	3. “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 private or secret information, Personal Data, Cardholder Data, commercially sensitive information, Critical Infrastructure Information, strategic business information, credentials, encryption data, system and application access logs, or any other information that may be subject to regulation.
	4. “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.
	5. “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.
	6. “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, omission or circumstance that compromises 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.
	7. “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 Breach, 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.
	8. “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).
	9. “Agreement” shall mean the Master Services Procurement Agreement, Master Materials Agreement or other agreement between CUSTOMER and VENDOR with respect to which this Rider is being entered.
3. 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.
4. Regarding the Processing of Personal Data and Company Data, the parties agree that:
	1. VENDOR shall Process Personal Data and Company Data only 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, (i) VENDOR shall not Process Personal Data or Company Data for any commercial purpose other than providing the services specified in the Agreement nor for any purpose outside the scope of the Agreement; and (ii) selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, Personal Data or Company Data for valuable consideration is prohibited.
	2. With regards to Personal or Company, the parties agree that:
* The Processing activities that will be carried out by VENDOR are: [How the third party will access the data].
* The categories of Personal or Company Data that will be Processed by VENDOR are: [Please review Data Classification Rule].
* The categories of Personal Data subjects whose information will be processed by VENDOR are: [insert categories].
* The instructions for the Processing of Personal or Company Data are: [insert instructions].
	1. 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.
	2. 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.
1. 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, (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.
2. At all times during which VENDOR is Processing Personal Data or Company Data, VENDOR shall:
	1. 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;
	2. 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:
		* 1. 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;
			2. The categories of Processing activities carried out on behalf of CUSTOMER;
			3. 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;
			4. 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;
	1. 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 Breach, including, without limitation, a Data Security 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. VENDOR shall implement Technical and Organizational Measures to ensure a level of security appropriate to the risk, taking into account the state-of-the-art, the costs of implementation, and the nature, scope, context and purposes of Processing, as well as, in connection with Personal Data, the risks of varying likelihood and severity for the rights and freedoms of data subjects. Without limiting the generality of the foregoing, the VENDOR will implement measures to:
1. Ensure the continued confidentiality, integrity, availability and resilience of Processing systems and services;
2. Quickly restore availability and access to Personal Data and Company Dara in the event of a physical or technical incident;
3. Verify and evaluate, on a regular basis, the effectiveness of the Technical and Organizational Measures implemented;
4. Pseudonymize and encrypt Personal Data, where applicable; and
5. Safely secure or encrypt all Sensitive Personal Data, Critical Infrastructure Information and other information that relates to the operation or functionality of plants, factories, networks, or grids of the CUSTOMER or its affiliates or to which they have access, during storage or transmission;
	1. 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.
	2. Notify CUSTOMER no later than one (1) day from the date of obtaining actual knowledge of any Data Security Breach, or from the date the VENDOR reasonable believes that a Data Security Breach 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 Breach involves Personal Data, the following information shall be provided as a minimum:
6. Description of the nature of the Data Security Breach, including, where possible, the categories and approximate number of data subjects affected, and the categories and approximate number of Personal Data records affected;
7. Contact details of the data protection officer of the VENDOR, where applicable, or other contact person for further information;
8. Description of the possible consequences of the Data Security Breach or violations; and
9. Description of the measures taken or proposed to remedy the Data Security Breach, including, where appropriate, the measures taken to mitigate possible negative effects;
	1. Assist and cooperate with CUSTOMER to enable CUSTOMER to comply with its obligations under any applicable privacy or security law, including but not limited to maintaining Personal Data and Company Data secured, responding to Data Security Breaches, and, where applicable, ensuring the rights of data subjects and carrying out Personal Data impact assessments;
	2. 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;
	3. 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;
	4. 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;
	5. 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.
	6. Establish policies and procedures to provide all reasonable and prompt assistance to CUSTOMER in responding to 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;
	7. 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;
	8. 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;
10. 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.
11. 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;
12. 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;
13. VENDOR shall cease Processing Personal Data and Company Data and return, delete, or destroy, or cause or arrange for the return, 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 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.
14. 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:
	1. 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”).
	2. 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.
	3. 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.
	4. 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.
15. 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 (as defined by ISO 27001/27002); and (b) any security requirements, obligations, specifications, or event reporting procedures set forth in Schedule A.
16. 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.
17. 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.
18. 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*]

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

|  |  |
| --- | --- |
| CUSTOMERBy: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Name: Title: Date: | VENDORBy: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Name: Title:Date: |
| By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Name: Title:Date: |  |

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

Schedule A

**General Security Requirements**

1. The following definitions are relevant to this General Security Requirements Schedule:
	1. “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.
	2. "Protected Information" means Personal Data and Company Data as defined in the Rider.
	3. Capitalized terms not otherwise defined in this Schedule shall have the meaning set forth in the Rider.
2. 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 Breach 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.
3. 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 security incident.
4. 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 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.
5. 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.
6. 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.
7. 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:
8. 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;
9. 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
10. 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.
11. 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:
12. 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
13. The same security measures shall apply to backups as to the original Protected Information.
14. 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 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:
15. Automatic locking if the device is left unattended for a certain period of time. User authentication will be required for unlocking.
16. Protection against malicious software and known vulnerabilities.
17. 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.

1. 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.

1. 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.
2. 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:

1. The VENDOR shall provide evidence or certificates that guarantee design security, firmware/software updates and malware protection.
2. The VENDOR shall conduct periodic analyses of vulnerabilities and inform CUSTOMER about any necessary updates, especially those that affect security.
3. All internet connected devices shall be protected with adequately complex passwords that can be changed by CUSTOMER.
4. 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.
5. 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:
	1. 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;
	2. Implement robust network and host-based monitoring solutions that looks for known malicious activity and anomalous behavior on the infrastructure and systems providing client services;
	3. Ensure that log information is aggregated and correlated to enable maximum detection capabilities, with a focus on monitoring for account misuse; and
	4. Work with CUSTOMER to ensure hosted infrastructure is monitored and maintained, either by the service provider or the client.
6. The VENDOR shall implement a procedure to notify of and manage any Data Security Breach or security incidents, which it will disclose among its Personnel, and will act with special diligence in those cases involving critical elements of CUSTOMER's Cyber-infrastructure or Protected Information or when the reputation or legal responsibility of CUSTOMERS or the interests of the persons whose information is Processed may be affected.
7. The Supplier shall immediately notify CUSTOMER of the existence of any security incident, even if it does not qualify as Data Security Breach, always within a maximum period of one (1) day after becoming aware of it, or if shorter, the shortest legal period, and shall assist and cooperate with CUSTOMER in terms of any necessary communication to third parties and other reasonable measures to remedy the situation when CUSTOMER requests it or as required by law.

 Merely by way of example, the Supplier shall notify CUSTOMER the following:

1. Access or attempts to access systems, equipment, applications, files, repositories, devices etc. by unauthorised persons or programs.
2. Disclosing or compromising protected Information including but not limited to credentials, authentication or encryption data.
3. Total or partial loss of data or information for any reason.
4. Uncontrolled distribution: sending information to people who should not receive it.
5. Loss or removal of computer equipment or storage media, files, repositories or part of their contents.
6. Attacks caused by viruses / malicious software that may affect the exchange of information between the VENDOR and CUSTOMER.
7. Others: any irregularity or deficiency detected regarding compliance with the safety criteria indicated in this Schedule.

Schedule B

**Cyber-Insurance Requirements**

1. VENDOR shall during the term of the Agreement have and maintain the following insurance coverage:
2. 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:
3. violations of data privacy or data security laws and regulations; and
4. 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
5. other risks specific to the work performed by VENDOR as shall be identified by CUSTOMER.
6. 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.
7. 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.
8. 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.

Schedule C

**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 Devicesowned 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.
		- 1. **Requirements and Practices**
	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. The determining authority and responsibility for issuance of an Electronic Device shall rest with the Avangrid Business Area Leader (BAL) or department hiring manager.
		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. 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.

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.

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:

##### Protecting Avangrid assets from unauthorized access and use by others,

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

##### Not leaving Electronic Devices in plain view in unattended vehicles,

##### Not leaving Electronic Devices in vehicles overnight,

##### Carrying laptops as hand luggage when traveling,

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

##### 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. 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. User shall follow Avangrid procedures for the return of Avangrid owned Electronic Devices when the use of those devices is deemed no longer necessary.
			- 1. 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.
		2. 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. **Connection to Avangrid Cyber-infrastructure**

### 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.

1. Non-Avangrid approved Electronic Devices shall not connect directly to the Avangrid Cyber-infrastructure (e.g. through Ethernet connection).
2. Wireless connections from an Avangrid office shall only be accomplished through Avangrid Electronic Devices and the Avangrid supported wireless infrastructure.
3. Guest wireless network accounts shall only be supplied on ‘as-need-be-basis’ following Avangrid approval processes.
4. Remote desk connections shall only be supplied on ‘as-need-be-basis’ following Avangrid approval processes.
	1. **Use of Mobile Devices (for Remote Access)**

### 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.

1. 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).
2. At no time shall a remote User initiate two simultaneous connections to different networks (e.g., no split tunneling and no multi-homed connection).
3. Avangrid issued SIM cards shall not be swapped or used in non-Avangrid issued Electronic Devices.
4. Configuring a non-Avangrid issued Electronic Device for connection to the Avangrid corporate email system is strictly prohibited.
5. Users should be aware that Avangrid may monitor emails sent from and to non-Avangrid issued devices.
	1. **Personally Owned Devices**

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

* 1. **Treatment of Software and Applications**

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

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

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

### 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.

### 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.

1. 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. **Treatment of Information/Data**

### 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.

### 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.

### 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.

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

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

### 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).

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

1. 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).
2. Discarded, when no longer needed, based on criticality, e.g. confidential and/or sensitive hardcopy shall be shredded.
3. To be removed from printers, fax machines, copier rooms, and conference/ meeting rooms immediately.
	1. **User Access Credentials and Passwords**

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

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

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

1. Privileged User IDs shall be reviewed and confirmed at least semi-annually.
2. Regular professional activities shall not be performed from a privileged ID.

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

1. Not sharing or disclosing their Avangrid credentials (log on IDs-user names and/or passwords) with others inside or outside the company.
2. Keeping secret authentication information confidential, ensuring that it is not divulged to any other parties, including senior management and technical support.
3. 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.
4. Changing secret authentication information when there is any indication of a possible compromise.
5. Reporting any incidents or suspected compromises by following Avangrid incident reporting procedures.
	1. **Internet Use and Social Media**

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

1. 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.
2. Access to restricted websites shall be enabled at the discretion of Avangrid and shall be provisioned following the security exception process.
3. Only Avangrid approved surfing software shall be used to access the Internet.

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

1. Accessing or posting of any racist or sexual content or any material that is offensive or defamatory in nature.
2. Accessing games, downloading video, music (MP3 or another format), or downloading any other files not related to the Avangrid related responsibilities.

### Limited and occasional use of Avangrid Electronic Devices and resources to engage in Social Networking[[1]](#footnote-2) and Blogging[[2]](#footnote-3) is acceptable, provided that:

1. It is done in a professional and responsible manner.
2. It does not violate the Code of Ethics or any relevant Avangrid policy, procedure or rule.
3. It is not detrimental to Avangrid’s best interests.
4. It does not interfere with regular work duties.
5. There is no breach of the prohibitions identified in these requirements.

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

* 1. **E-mail Use**

### 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.

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

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

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

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

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

1. Use does not interfere with the normal performance of professional duties.
2. Messaging does not violate applicable laws, regulations, the Code of Ethics, or Avangrid policies.
3. Use is moderate both in terms of frequency and amount of memory and resources consumed.

### 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’.

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

1. Harassing or discriminatory messages which relate to gender, race, sexual orientation, religion, disability or other characteristics protected by applicable laws and regulations.
2. Defamatory messages which adversely affect the reputation of a person or company.
3. Messages that violate copyright, trademark, trade secret or other intellectual property rights.
4. Obscene materials or images of a sexual nature.
5. 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.
6. Any material or images that might reasonably be expected to cause personal offense to the recipient.
7. Messages in violation of applicable laws, regulations, the Code of Ethics, or Avangrid policies.

### 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.

1. 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.

### 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. **Incident reporting**

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

* 1. **Contract Termination**

### 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.

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

* + - 1. **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.

* + - 1. **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.

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.

* + - 1. **Non Compliance**

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

1. Social Networking is the use of dedicated websites and applications to interact with other users or to find people with similar interests. [↑](#footnote-ref-2)
2. 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. [↑](#footnote-ref-3)