



## **MASTER MATERIALS PROCUREMENT AGREEMENT**

**THIS MASTER MATERIALS PROCUREMENT AGREEMENT** (“Agreement”) is made this 24<sup>th</sup> day of May 2021 (the “Effective Date”) by and between **Avangrid Service Company**, a Delaware Corporation, with offices located at One City Center, 5<sup>th</sup> Floor, Portland, Maine 04101. (hereinafter, “Company” or “Customer” or “AVANGRID”) and [REDACTED] (hereinafter, “Supplier” or “Vendor” or “Contractor” or “Insight”). Customer and Supplier may be referred to individually as a “Party” and collectively as the “Parties.”

### **WITNESSETH:**

**WHEREAS**, Customer is authorized to assist the utility operating companies set forth in *Schedule A*, attached hereto and made part hereof, in procuring certain products and materials and related services that they may require from time to time in the operations of their respective businesses, including the products and materials together with the associated services, each as described in *Schedule B*, attached hereto and made part hereof (the “Materials”); and

**WHEREAS**, the Supplier states that it is an established and well-known supplier of the Materials and is willing to provide the Materials to the companies in accordance with the terms and conditions of this Agreement; and

**WHEREAS**, in reliance upon such statements and following its review of Supplier’s proposal and negotiation of business terms, Customer has selected Supplier as a vendor-of-choice for the Materials, which shall be procured and performed in accordance with this Agreement.

**NOW THEREFORE**, in consideration of the mutual covenants contained herein, and other good and valuable consideration, Supplier and Customer hereby agree as follows:

### **1. DEFINITIONS**

As used in this Agreement:

- (a) “Affiliate” shall mean, with respect to a Party, any other entity Controlling, Controlled by, or under common Control with such Party. The term “Control” and its derivatives shall mean with regard to any entity, the legal, beneficial, or equitable ownership, directly or indirectly, of fifty percent (50%) or more of the capital stock (or other ownership interest, if not a Corporation) of such entity ordinarily having voting rights.
- (b) “Company” and its derivatives shall mean the Affiliates of Customer specified in *Schedule A*, attached hereto and made part hereof.

- (c) “Contract Price” shall mean, in the aggregate, the total maximum dollar amount of all the Materials pursuant to this Agreement, including, without limitation, any amendment or other modification thereto.
- (d) The “Effective Date” shall mean the date specified in the recitals of this Agreement.
- (e) “Materials” shall mean the products, goods, materials, equipment, parts, software and its related maintenance and support, third party branded services, the information technology and professional services and/or other items and other services described in **Schedule B**, attached hereto and made part hereof. For purposes of this Agreement, the services component of the Materials does not include third-party branded services, Software as a Service (“SaaS”), or other cloud computing offerings.
- (f) “Purchase Order” shall mean a purchase order issued by Customer or a Company in accordance with this Agreement.
- (g) “RFP” shall mean a request for proposal for the Materials, which shall include a reasonably detailed description of the Materials required by the Company(ies), volumes, delivery requirements, and other terms relevant to the purchase.
- (h) “Term” shall mean the term of this Agreement, as extended or terminated early in accordance with this Agreement.
- (i) “Terms and Conditions” shall mean the terms and conditions, the form of which are set forth hereto in **Schedule C** and made a part hereof and which govern the purchase of Materials and related matters pursuant to a Purchase Order.
- (j) “Small Business Concern” as defined by the Small Business Administration, shall mean a business that is independently owned and operated and which is not dominant in its field of operation. The law also states that in determining what constitutes as small business, the definition will vary from industry to industry to reflect differences accurately.
- (k) “Statement of Work” or “SOW” is an order for all or a portion of the Materials issued in accordance with this Agreement, including, without limitation, any related service components, which is prepared by Supplier pursuant to the terms herein and submitted to Customer but shall not be effective until mutually agreed upon in writing by the Parties.

## 2. **PROCESS FOR PURCHASING MATERIALS**

- 2.1 Customer agrees that, upon a request made to Customer by a utility operating company for assistance in procuring Materials, Customer shall, on its own or with the assistance of the Companies requiring the Materials, take either of the steps delineated in subsections (a) or (b):

(a) Issuance of Purchase Order. Customer or the Company(ies) requesting the Materials shall issue to the Supplier duplicate originals of a Purchase Order for the Materials written against a SOW for the Materials incorporating: (i) the specifications set forth in **Schedule B**, (ii) the Terms and Conditions set forth in **Schedule C**, (iii) the pricing terms set forth in **Schedule D**, and (iv) Material volumes, delivery requirements, and other terms relevant to the purchase. Upon receipt of an authorized Purchase Order for the Materials and a fully executed SOW, Supplier shall acknowledge the order and commence fulfillment of the order in accordance with the terms therein.

OR

(b) Issuance of an RFP. (i) Customer or the Company(ies) requesting the Materials shall issue an RFP to the Supplier. Within the time period specified in the RFP, Supplier shall issue a written proposal to Customer, or, if so directed, to the Company specified in the RFP, setting forth: (1) a detailed description of the Materials to be provided by the Supplier, consistent with the specifications and other requirements specified in the RFP, and (2) Supplier's pricing and charges for the Materials, which Supplier warrants will be calculated in accordance with the pricing terms set forth in **Schedule D**, attached hereto and made part hereof.

(ii) Within the time period specified in the RFP, Customer and/or the Company(ies) shall review the Supplier's proposal. If Customer and the Company(ies) requiring the Materials, in their sole and absolute discretion, determine that they wish to award a contract for Materials and thereupon select the Supplier's proposal, the Company may elect to issue a Purchase Order and (in such instance) Company shall forward duplicate original Purchase Orders for the Materials (conforming with the requirements of Section 2.1(a), above and a SOW for the delivery and performance of the Materials, but also incorporating the Supplier's proposal in accordance with this Agreement) to the Supplier at the address specified in **Schedule F**, below. Upon receipt of an authorized Purchase Order, Supplier shall commence fulfillment of the order for the Materials and upon the issuance of a Purchase Order written against a SOW, will commence the Materials, in accordance with the terms therein.

**2.2** (a) Notwithstanding anything to the contrary in this Agreement or in any Purchase Order, SOW, or RFP issued hereunder, Customer make no representation or warranty that Customer or any of the Companies will issue any Purchase Orders, SOWs, or RFPs, or any minimum dollar volume of Purchase Orders, SOWs, or RFPs, during the Term. Customer or the Companies requesting Materials and/or services may terminate a Purchase Order, SOW, or RFP for such Materials prior to commencement of fulfillment of the Purchase Orders for such Materials and in accordance with the SOW at any time upon written notice, without penalty or other obligation, prior to commencement of fulfillment of the Purchase Orders for such Materials.

(b) Supplier acknowledges and agrees that the issuance of an RFP, Purchase Order, SOW, or other document pursuant to this Section 2 by Customer or any Companies shall not constitute an offer by Customer or any Companies to purchase Materials, and that an enforceable agreement for Materials shall result only when Supplier commences fulfillment of the Purchase Order for such Materials or the SOW.

(c) Supplier further acknowledges that each Purchase Order for the Materials and SOW processed in accordance with this Section 2 and issued to Supplier by Customer or a Company constitutes a separate and distinct contract for the particular Materials identified in the Purchase Order or in the SOW and shall be governed by the following documentation:

- (i) The Purchase Order (exclusive of its pre-printed terms and conditions) for the Materials to be purchased by Customer/Company or the SOW for the Material to be procured and performed by Supplier for Customer/Company;
- (ii) Special Conditions and SOW attached hereto as *Schedule E*;
- (iii) The Terms and Conditions attached hereto as *Schedule C*, as they may be amended or modified for the particular Purchase Order;
- (iv) The Data Security Rider attached hereto as *Schedule H*;
- (v) The Insurance requirements attached hereto as *Schedule G*;
- (vi) The Materials document attached hereto as *Schedule B* for the Materials, as it may be amended, modified or supplemented for the particular Purchase Order; and
- (vii) This Agreement, including all Schedules other than those described in subsections (i), (ii), (iii), (iv), (v), and (vi) above.

In the event of any inconsistency among the aforementioned documentation, the order of precedence shall be as set forth in subsections (i), (ii), (iii), (iv), (v), (vi) and (vii), above.

### **3. PRICING; PAYMENT; DISCOUNTS AND REFUNDS**

- 3.1** (a) Supplier agrees that pricing, fees, pass-throughs, and other charges set forth in *Schedule D* will be incorporated into and used as the basis for all pricing, fees, pass-throughs, and other charges in: (i) any proposal issued by Supplier hereunder, and/or (ii) any Purchase Orders pursuant to this Agreement.

(b) Supplier agrees that the pricing terms set forth in *Schedule D* shall be fixed for the time period specified in such Schedule and shall not be subject to increase except as expressly specified in such Schedule and if not specified, shall be fixed for one year from the Effective Date of this Agreement

**3.2** (a) Supplier agrees that, in calculating any discounts or adjustments to prices, fees, pass-throughs, and charges set forth in *Schedule D* that are based upon volumes or quantities of Materials purchased from the Supplier, Supplier shall include in such calculation the volumes or quantities of services for all Purchase Orders issued by Customer or any Companies pursuant to this Agreement during the relevant time period.

(b) Within thirty (30) days following each anniversary of the Effective Date of this Agreement, Supplier shall forward to Customer a draft reconciliation statement showing Supplier's calculation of any rebates or refunds payable as a result of the total value of all Purchase Orders for Materials issued by the Companies with the Supplier during the preceding calendar year. Customer shall review the reconciliation statement and will notify Supplier of any comments it may have with respect thereto within thirty (30)-days of its receipt thereof. Supplier shall pay to Customer the undisputed portion of any rebates or refunds due the Companies under executed Purchase Orders for Materials within five (5) business days following the earlier of: (i) Supplier's receipt of the comments of Customer and Companies, and (ii) the thirty (30) day period referenced in the immediately preceding sentence.

#### **4. NO GUARANTY; HOLD HARMLESS**

Supplier acknowledges and agrees that, notwithstanding anything to the contrary contained in this Agreement, any subsequently issued RFP, or in any Purchase Order between Supplier and any Company, that with respect to any Purchase Order for Materials issued by any Company pursuant to this Agreement:

(a) All charges, fees, and expenses, as well as any credits, refunds, or rebates, resulting from Materials sold by Supplier pursuant to such Purchase Orders shall be solely for the account of such Company, and neither Customer nor any other Companies shall be considered a guarantor or surety of any charges, fees, and expenses arising under such Purchase Order;

(b) All communications, notices, invoices, and reports resulting from Materials sold by Supplier pursuant to such Purchase Order shall be directed to the representative(s) of the Company identified in such Purchase Order;

(c) Supplier covenants not to sue Customer or any other Company, except for the Company issuing the Purchase Order, for any charges, fees, expenses, or claims arising from or attributable to Materials sold by Supplier pursuant to such Purchase Order; and

(d) Pursuant to Article 13 of *Schedule C*, Supplier shall hold Customer and the other Companies and their respective employees, agents, officers, shareholders, directors, affiliates, managers, directors, members, partners, successors, and permitted assigns harmless from and against any and all damages or liabilities arising from or attributable to, directly or indirectly, the performance, non-performance, or other negligent acts of the Supplier and its employees, agents, or representatives pursuant to such Purchase Order.

## 5. TERM

5.1 This Agreement shall be effective as of the Effective Dates and shall remain in effect for a three (3) year term, unless earlier terminated according to section 5.2 below.

5.2 (a) Customer may terminate this Agreement at any time and for any or no reason in accordance with the terms of Articles 16 and 17 of *Schedule C* to this Agreement. Upon the effective date of termination specified in Customer's termination notice: (i) all RFPs, proposals, and Purchase Orders or SOWs then in process, but for which Supplier has not begun fulfillment shall be deemed canceled, unless otherwise agreed in writing by the Company(ies) requesting or issuing such RFPs, proposals, SOWs, and/or Purchase Orders, and (ii) this Agreement shall be terminated without liability or obligation to the Parties, except for any liabilities and obligations of Supplier arising under any previously fulfilled Purchase Orders/SOWs. Customer shall have no liability for any costs, expenses, or other fees incurred by Supplier in connection with any RFPs, proposals, or Purchase Orders that are in process but not fulfilled upon the effective date of termination of this Agreement by Customer.

(b) Termination of this Agreement by Customer shall not effect, or result in, termination of any Purchase Orders or SOWs where Supplier has begun to fulfill the orders thereto prior to the effective date of termination set forth in Customer's termination notice; provided, however, that this subsection (b) shall not constitute a waiver or relinquishment of any right of termination of any Company pursuant to the terms and conditions of such Purchase Orders or SOWs.

## 6. GENERAL


6.1 Notices. All notices, requests, demands, and determinations under this Agreement shall be in writing and shall be deemed duly given: (i) when delivered by hand, (ii) one (1) day after being given to an express courier with a reliable system for tracking delivery designating overnight delivery, (iii) when sent by confirmed facsimile with a copy sent by another means specified in this Section 6.1, or (iv) six (6) days after the day of mailing, when mailed by United States mail, registered or certified mail, return receipt requested, postage prepaid, and addressed to the Party at the address(es) specified in *Schedule F* to this Agreement. A Party may from time to time change its address or designee for notification purposes by giving the other prior written

notice of the new address or designee and the date upon which it will become effective.

- 6.2** Governing Law. This Agreement and performance under it, and all actions, causes of action, or claims of any kind (whether at law, in equity, in contract, in tort, or otherwise), shall be governed by and construed in accordance with the laws of State of New York, including without limitation New York laws relating to applicable statute of limitation and burdens of proof and available remedies.
- 6.3** Binding Nature and Assignment. This Agreement shall be binding on the Parties hereto and their respective successors and assigns. Neither Party may, or shall have the power to, assign this Agreement without the prior written consent of the other, and any such attempted assignment without such consent shall be null and void, except that Customer may assign this Agreement and its rights and obligations hereunder to an Affiliate without the approval of the Supplier, but on prior written notice.
- 6.4** Entire Agreement; Amendment. This Agreement, including any Schedules referred to herein and attached hereto, each of which is incorporated herein for all purposes, constitutes the entire agreement between the Parties with respect to the subject matter hereof and supersedes all prior agreements, whether written or oral, with respect to the subject matter contained in this Agreement. No change, waiver, or discharge hereof shall be valid unless in writing and signed by an authorized representative of the Party against which such change, waiver, or discharge is sought to be enforced.
- 6.5** Counterparts. This Agreement may be executed in several counterparts, all of which taken together shall constitute one single agreement between the parties hereto.
- 6.6** Headings. The article and section headings and table of contents used herein are for reference and convenience only and shall not enter into the interpretation hereof.
- 6.7** Relationship of Parties. Supplier is not an agent of Customer and has no authority to represent Customer or the Companies as to any matters, except as expressly authorized in this Agreement.

IN WITNESS WHEREOF, Customer and Supplier have each caused this Agreement to be signed and delivered by its duly authorized representative as of the date first given above.

**Avangrid Service Company**

DocuSigned by:  
  
099C68F11EAG4E...

Signature

Peter Church

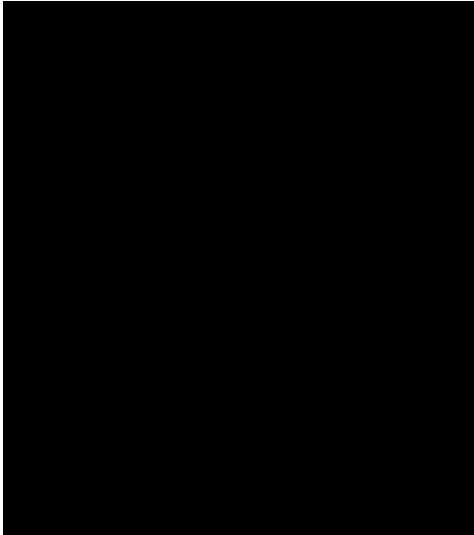
Print Name

Chief HR Officer

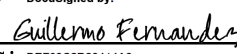
Title

6/11/2021

Date



**Avangrid Service Company**

DocuSigned by:  
  
DEF8927D8D14AG...

Signature

Guillermo Fernandez

Print Name

Controller - Corporate Functions

Title

6/11/2021

Date



**SCHEDULES:**

- Schedule A: Companies
- Schedule B: Materials
- Schedule C: Terms and Conditions
- Schedule D: Pricing Terms
- Schedule E: Special Conditions
- Schedule F: Notices
- Schedule G: Insurance Requirements
- Schedule H: Data Security Rider
- Schedule I: Background Check Requirements



**SCHEDULE A**

Companies

**Central Maine Power Company**

Augusta General Office  
83 Edison Drive, Augusta, Maine 04336

**New York State Electric & Gas Corporation**

89 East Avenue  
Rochester, New York 14649

**Rochester Gas and Electric Corporation**

89 East Avenue  
Rochester, New York 14649

**The Berkshire Gas Company**

115 Cheshire Road  
Pittsfield, MA 01201

**Maine Natural Gas Corporation**

4 Industrial Parkway  
Brunswick, ME 04011

**UIL Holdings Corp.**

180 Marsh Hill Rd, Orange, CT 06477

**The United Illuminating Company**

**Ops Center**

100 Marsh Hill Rd, Orange, CT 06477

**The Southern Connecticut Gas Company**

Locations:

**SCG Ops Center**

Southern Connecticut Gas  
60 Marsh Hill Rd, Orange, CT 06477

**SCG LNG**

775 Oronoque Rd, Milford, CT 06461

**Connecticut Natural Gas Corporation**

Locations:

**CNG LNG**

1376 Cromwell Ave, Rocky Hill, CT 06067

**CNG Ops Center**

East Hartford

76 Meadow Street, East Hartford, CT 06108

## **SCHEDULE B**

### **Materials**

#### **1 TECHNOLOGY SOLUTION DESCRIPTION**

There is a need for the network to support new, higher-bandwidth packet-based services as well as legacy TDM services (for the foreseeable future). The network shall support an aggregation of mixed services from different applications (teleprotection, CCTV, alarms, telephony, LMR, SCADA, Wi-Fi, internet traffic etc.). These services shall access the IP/MPLS equipment using Ethernet connectors through third party interface adapters when required. Optionally, the access network shall support different types of physical interfaces including T1 TDM, Ethernet, serial, and legacy or specific interfaces such as FXO/FXS, E&M, and IEEE C37.94. In such a network, it shall be possible to both connect remote devices to central SCADA servers using TDM or IP networks, as well as optimize data transport for teleprotection among substations. The network needs to support optimized traffic delivery for multicast applications as well as traditional data transport for all traffic. AVANGRID will select the interfaces to be deployed at each stage, and how to build the network.

To benefit from the advanced resiliency, traffic isolation, and traffic engineering features of IP/MPLS, the solution will need to use a full IP/MPLS network, from all remote locations up to Control Centers.

The main features and relevant data of the technology solution to be quoted are provided in the requirements and technical specifications described through this document.

The technology to be implemented must provide a homogeneous end-to-end MPLS architecture. That is, from any access node to any other, through the core network, MPLS technology must be available.

For routing purposes, two types of nodes are defined, so the necessary equipment shall be provided depending on its functionality in the network:

- Core Routers. They support the network backbone. They also have the possibility to support access to services when location and distance allow it.
- Access Connection Routers. They access the services to the core network through a transport network or by a direct connection taking advantage of available optical fibers. Each Access Connection Router is redundantly connected to two different Core Routers.

#### **1.1 SERVICE REQUIREMENTS**

All services will start to be migrated to native Ethernet/IP. The current and future potential services to be carried over the network are as follows:

<b>Service</b>	<b>Interface</b>	<b>Notes</b>
Video surveillance/CCTV Access control Intercom	Ethernet/IP	All these services are unicast
Intra-substation communication	Ethernet	IEC 61850
SmartGrid applications	Ethernet/IP	AMI and other
Corporate IP network	Ethernet/IP	
Corporate voice network	Ethernet/IP	VoIP

## 1.2 CURRENT NETWORK

The current AVANGRID network consists of a SONET backbone operating on OC-48 links with OC-3/OC-12 access rings backhauling traffic between substations as well as back to the Control Center. Microwave radios and services leased from local carriers are also used. Local TDM-based multiplexers terminate T1, n x 64 kbps as well as sub 64 kbps interfaces. IP routers provide corporate IT access. The IT network routers typically interface directly with SONET equipment via Ethernet interfaces.

At present, only transmission substations have comprehensive monitoring and control capabilities. The distribution substations have a single SCADA link over RS-232 serial or 4W analog service. However, the 4W analog leased-line service from the local carriers is being discontinued.

## 1.3 FUTURE NETWORK

The AVANGRID WAN Network must be a NERC CIP Version 5 compliant operational telecommunications system with the following specifications

- Highly scalable, end-to-end solution
- High availability and reliability
- Robust synchronization
- Equipment shall be hardened to utility requirements
- Secure – Meets NERC CIP recommendations
- Future-proof capabilities
- Evolution to SDN
- Integrate all AVANGRID services onto single network for cost/operational efficiencies

As mentioned before, some selected legacy TDM systems still need to be supported during the migration period. These systems will be combined with high bandwidth packet-based services on a converged transport network. The solution will use a DWDM transport core with a full IP/MPLS network overlay, from AVANGRID Networks locations to Data centers.

Legacy TDM and associated traffic (e.g. SONET) will be transported directly over the new DWDM optical infrastructure and the IP/MPLS backbone.

Traffic will be carried using several types of VPN services such as:

- VLL point-to-point service for traditional TDM, Ethernet, and non-IP services using PWE3 pseudowires.
- VPLS point-to-multipoint service allowing transparent transport of data at Layer 2, to minimize complexity.
- VPRN
- IP multicast delivery.

IP/MPLS traffic will be carried over a transport network which is composed of:

- A DWDM fiber optic infrastructure based on dark fiber (leased from local carriers) connecting various locations,
- A DWDM fiber optic infrastructure based on fiber optic cables owned by AVANGRID
- Ethernet leased lines (e.g. 10 Gbps)

A network management system (NMS) including fault analysis, performance management, provisioning of network and network devices, maintaining the quality of service will be implemented to give a 360-degree view of the IP/MPLS network.

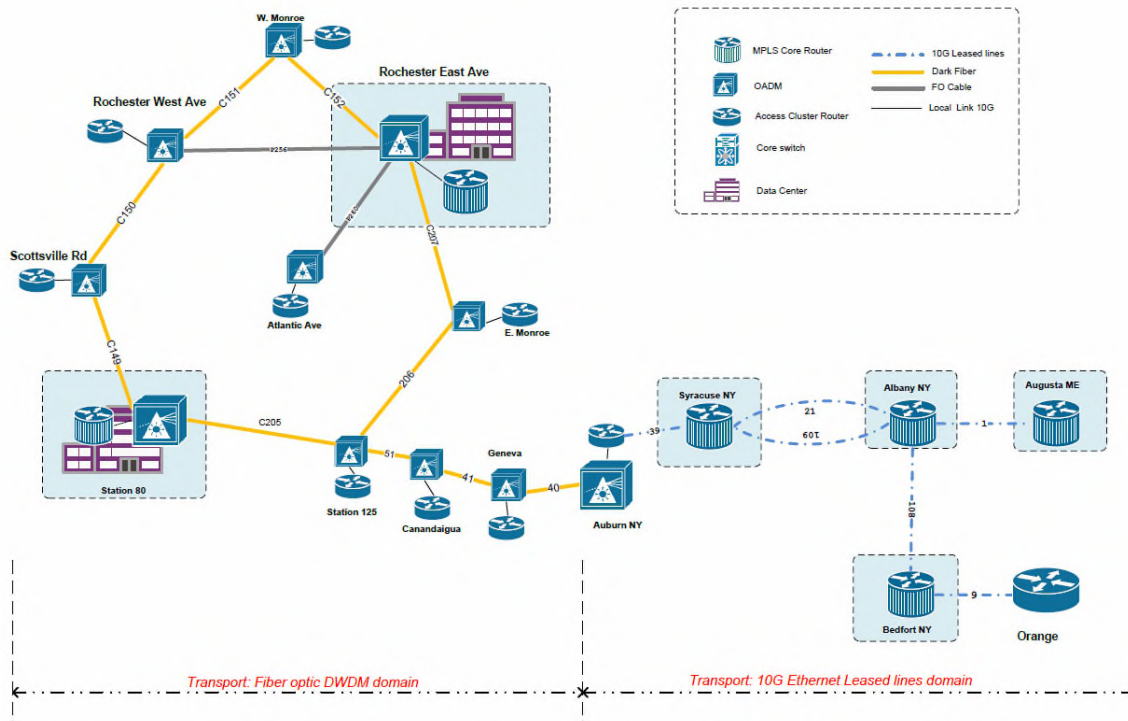


Figure 3: Pilot IP/MPLS Network

The IP/MPLS equipment already deployed consists of Nokia 7705 SAR-8 and 7750 SR.

#### 1.4 SECURITY STRATEGY

In every site, a stateful firewall working in transparent mode shall be installed inspecting all ingress and egress traffic, so, IP/MPLS equipment with firewall capabilities will be positively valued.

## 2 REQUIRED TECHNICAL FEATURES AND PERFORMANCE

**IP/MPLS Core routers** – Central core of large capacity routers located at Control Centers and major locations. The backbone between the routers shall be based on multiple instances of 1 Gbps, or 10 Gbps links. These shall be large, highly scalable devices capable of 40/100 Gbps operations.

**IP/MPLS Access cluster routers** – Primarily located at transmission substations as well as in the distribution network, distribution substations, and at remote distribution automation cabinets as points of traffic aggregation. There is significant legacy TDM equipment present, providing monitoring and control of transmission and generation power facilities.

### 2.1 EQUIPMENT MAIN FEATURES

#### 2.1.1 Core router

\*For Section 2, please see Exhibit B3 below, Compliancy Grids\*



Exhibit B3.

Compliancy Grids.xlsm

Main Features:

- There will be a minimum of 8 slots in the chassis
- The equipment shall operate either as an MPLS LSR or LER
- The availability of the interface type as well as modularity (# ports/card) and system capacity of each interface shall be provided
- All cards in the chassis shall be hot-swappable
- LAG with 10 Giga interfaces.
- BFD and IEEE 802.3ah.
- IGP OSPF.
- MP-BGP.
- MPLS FRR.
- QoS with 8 FC.
- VPLS: 2,000 instances.
- VPRN: 140 instances.
- VPRN routes per instance: 300,000 routes.

It shall support a minimum density per device of:

- 48 x 1GbE Optical
- 24 x 10GbE Optical
- 6 x 100GbE Optical

#### 2.1.2 Access Router

Main features:

- There shall be a minimum of 6 slots in the chassis for line cards
- The equipment shall operate either as an MPLS LSR or LER

- The availability of the interface type as well as modularity (# ports/card) and system capacity of each interface should be provided
- All cards in the chassis should be hot-swappable
- LAG with 10 Gbps interfaces.
- BFD and 802.3ah.
- IGP OSPF.
- MP-BGP.
- MPLS Fasterroute.
- QoS with 8 FC.
- VPLS: 20 instances.
- Routed VPLS.
- VPRN: 20 instances.
- VPRN routes per instance: 2,000 routes.

It shall support a minimum density per device of:

- 4 x 10GbE (optical)
- 48 x 1GbE
- 24 x 10GbE (colocation sites and offices) \*MX104 has 12 x 10gbe ports\*
- 4x 10GbE (transmission and distribution substations)

Both kind of equipment shall

- Use -48 VDC for power
- Be 19'' rack compatible
- Allow Front access
- Be able to operate under the following environmental conditions:
  - 0°C to +65°C sustained operation
  - -40°C to +70°C shipping and storage
  - 5% to 95% humidity (non-condensing)

## 2.2 THROUGHPUT CAPACITY

The vendor shall describe in detail the traffic throughput capacity of the equipment and each of its components.

- a. Processing type (centralized or distributed). If any card has any limiting characteristics, it should be stated.
- b. General throughput capacity (Gbps).
- c. Backplane capacity (Gbps).
- d. Capacity per slot (Gbps).

## 2.3 AVAILABILITY AND REDUNDANCY

The proposed **IP/MPLS Core** and **Access routers** shall support redundancy at the following level:

- Control / switch fabric
- Redundant power inputs

- Fans
- Non-stop routing
- Non-stop forwarding

## 2.4 INTERFACES

The availability of the interface type as well as modularity (# ports/card) and system capacity of each interface should be provided.

Indicate if all the supported cards including control, power and fans are hot swappable.

### 2.4.1 Ethernet Interfaces

The proposed **IP/MPLS Core and Access routers** shall support:

- 10/100 Fast Ethernet (optical and electrical)
- 100/1000 Gigabit Ethernet (optical and electrical)
- 10Gbps Ethernet (optical)

Additionally, the proposed **IP/MPLS Core router** shall support:

- 40Gbps Ethernet

The types of the optical and electrical SFPs available for the various interfaces shall be specified.

## 2.5 MPLS

This functionality is mandatory and should be based on the IETF and MPLS Forum standards. It is necessary to specify the protocol standards (IEEE, IETF, etc.) and versions that apply for the aspects listed below. In case of having any proprietary non-standard implementation, it must be specifically indicated, and its added value shall be explained.

The aspects that should be considered are:

- a. Use of OSPF as IGP.
- b. Use of IS-IS as IGP.
- c. Definition of LSP manually, strictly defining primary and secondary path, and last path as loose.
- d. LSP signaling by RSVP-TE. Indicate if there are any restrictions.
- e. Fast-reroute support.
- f. Indicate the maximum number of RSVP-TE LSP's. Maximum number of LSP's (Head End), Maximum number of LSP (Transit). Maximum number of LSP's (Egress).
- g. Possibility of defining SDP indicating the LSP, or using LDP.
- h. Use BGP for community use in VPRNs.
- i. Indicate the number of Core Routers at which it is considered necessary to start using Route Reflectors.
- j. iBGP peering should be possible against at least two "Route Reflector".
- k. Specify interoperability with third party equipment.

## 2.6 QoS

QoS support is mandatory and has to comply with RFC 5462.



It is necessary to specify the protocol standards and versions for each of the following aspects. In case of having any proprietary non-standard implementation it must be indicated, its added value shall be explained:

- a. QoS support on all types of interfaces.
- b. EXP-based QoS: traffic shaping is done at the markup level and the assignment to a service queue is done directly at the input, based on the MPLS EXP header.
- c. Describe in detail the processes of: classification, marking, queuing and scheduling.
- d. The classification will be made according to 8 qualities of service levels (Forwarding Class - FC).

	FORWARDING CLASS
HIGH PRIORITY	NC
	H1
	EF
	H2
LOW PRIORITY	L1
	AF
	L2
	BE

- e. The queues can be characterized by CIR, PIR, CBS and MBS. Modification of CBS and MBS is due to delay-sensitive traffic.
- f. It is necessary to have implemented a hierarchical scheduler, due to the need to share different types of traffic in one SAP. Three levels.
- g. Traffic classification by SAP towards FC in MPLS.
- h. Traffic classification by CoS towards FC in MPLS.
- i. Traffic classification by ToS (DSCP) towards FC in MPLS.
- j. Traffic classification by IP range, origin or destination, towards FC in MPLS.
- k. Rewriting capability of CoS and ToS fields in the frames. It should be made both in inward/outward interfaces.
- l. Indicate if there is any limitation in terms of scalability between the number of queues and the number of SAP, per port, slot, chassis or physical interface.

## 2.7 NETWORK REDUNDANCY

In order to maintain a high level of availability in the network, there shall be a high level of equipment redundancy to protect against equipment failure. There shall also be higher-level network redundancy capabilities to protect against network failures such as fiber cuts and catastrophic node failures. The network redundancy requirements are listed below:

- LAG (active/standby, active/active)
  - Single and multi-chassis
- Active/standby pseudo-wires
- MPLS Fast Re-route (FRR)
- ECMP (LDP and IP)
- IP Fast Re-route (FRR)
- LDP Fast Re-route (FRR)
- BGP Prefix Independent Convergence (PIC)

- Pseudo-wire redundancy

## **2.8 SERVICES**

### **2.8.1 VPLS AND VLL**

These functionalities are mandatory: emulation of Ethernet services multipoint-to-multipoint (VPLS) or end to end (VLL-Virtual Leased Lines) through an MPLS network. VPLS service has to comply with RFC 4762. VLL service has to comply with RFC 4447.

### **2.8.2 VPRN**

This functionality is mandatory. Its implementation must be carried out according to the standards established by the IETF (RFC 4364) and the MPLS Forum.

### **2.8.3 TUNNELS**

While the network is based on IP/MPLS, the equipment shall also support encapsulation in GRE and IP, providing more flexibility to expand the network through third party networks if required.

### **2.8.4 SYNCHRONIZATION**

Synchronization is required to ensure proper transport of circuit emulated services as well as accurate time-of-day information for current and future IED's. The equipment shall have the ability to use the following synchronization sources listed below.

- Line timing:
  - T1/E1
  - T3/E3
  - SONET/SDH
  - Synchronous Ethernet (SyncE)
- GPS (internal to equipment or external)
- External or BITS timing
- IRIG-B
- In band packet-based timing
  - Adaptive clock recovery
  - IEEE1588v2 (slave, boundary clock and transparent clock)

### **2.8.5 LAYER 2/ETHERNET FUNCTIONALITY**

The proposed solution shall support the following functionalities:

- 10/100/1000 autosensing
- Encapsulation
- IEEE 802.1q VLAN
- IEEE 802.1ad Q-in-Q
- Jumbo frames (9 kbytes)
- LACP
- MAC filters
- 802.1b Link Layer Discovery Protocol (LLDP)
- Routed VPLS
- Unnumbered interface

- Ethernet ports should be capable of operating as network or access interfaces or a mix of both (hybrid port)

### **2.8.6 IP/LAYER 3 FUNCTIONALITY**

The proposed solution shall support the following functionalities:

- IPv4 and IPv6 support
- Routing protocols
  - Static
  - OSPF/OSPF3
  - IS-IS
  - MP-BGP
  - RIP
  - PIM multicast
- PE-CE support
  - BGP
  - RIP
  - OSPF
- VRF support
- DHCP (slave, server)
- IP ECMP

### **2.8.7 LOOPBACKS**

All physical interfaces (Ethernet and TDM) should have a physical loopback capability to loop the incoming traffic back to the source (line loopback) and loop the outgoing traffic back towards the switch fabric prior to exiting the equipment (equipment loopback).

### **2.8.8 SERVICE MIRRORING**

- Local/Remote
- IP
- Ethernet

### **2.8.9 ROUTE REFLECTORS**

Beyond what has been described above, those Access Routers designated as Router Reflectors shall support:

- 1,000 peers.
- Routes 600,000.

## **3 MANAGEMENT**

This section describes NMS requirements. The NMS shall be an effective set of hardware and software tools that are capable of supervising the AVANGRID telecommunications network, its individual elements and signaling protocols. The NMS is part of a larger network management framework (consistent with the commissioning of an OSS and a BSS platform). Implementation of the NMS will occur in three geographical areas for redundancy and backup.

. When availability and performance are required, the NMS shall assist in quickly identifying and resolving problems. The average repair time shall be as short as possible to avoid downtime.

The NMS platform itself shall be fully protected against attacks, including, but not limited to, the following:

- Active directory compromises
- SQL injection
- XML injection
- JavaScript injection
- Cross-site scripting
- Cross-site request forgery

The NMS shall be capable of managing all network devices, including peripherals and third party elements. The features of the NMS are as follows:

- A centralized architecture with high availability and continuity of service
- An integrated information platform containing inventory elements, users, and associated services
- \*Visibility of network capacity and health of network elements
- Rapid identification and location of problems
- Automation of management tasks
- Simplified integration of network devices, peripherals, and third-party elements
- Capacity to evolve in stride with technological advances
- Multivendor network equipment environment
- \*Mapping visualization
- Fixed and mobile device independent access
- Ease of third party OSS and BSS integration
- Secure
- High availability
- Network architecture independence
- Management of optical devices
- Service, system, network and route analytics

Overall, the NMS shall provide a universal solution for managing the telecommunications network while minimizing the number of interfaces and management platforms. The NMS shall be accessible via a highly secure web session from any location in the network. It shall facilitate the automated configuration of network elements, the simplified reconciliation of inventory data, and the collection of network traffic.

\*The NMS shall constantly monitor the telecommunications network for slow or failing network elements and notify the network administrator via email, or texting in the event of a performance degradation or outage.

The NMS shall automatically display the services associated with each network resource. The NMS should include route analytics to monitor the routing structure of the telecommunications network to prevent incorrect routing that could cause undesirable performance degradation.

\*In addition, the NMS shall be sufficiently open to allow information sharing with operational support tools. In particular, the NMS shall support standard external interfaces such as SNMP with MIB virtual databases, Web services, LDAP, etc. to be integrated with third party systems.

In summary, the NMS will enable AVANGRID to save time in integrating and troubleshooting network elements, prevent network disruption, document performance, and minimize security risks.

### **3.1 FAULT MANAGEMENT**

By monitoring the health of all electronic and optical network devices and components, the NMS shall detect, locate, isolate and correct malfunctions in the telecommunications network and its environment. It shall also assist network administrators in correcting faults in a timely manner.

Furthermore, it shall verify the performance of a network device with its fundamental parameters of operations and established service-level agreements. The NMS shall alert the appropriate staff through email, texting, and on screen messages when abnormal operations are detected. It will then trigger manual or automatic activities such as bringing backup systems on-line.

The NMS shall also carry-out maintenance phases, such as:

- Supervision of alarms
- Supervising the reliability of network elements
- \*Measurement of the continuity index and the availability of the telecommunications network as a whole and for each link
- \*Estimation of the survivability of services
- Integration of troubleshooting tools with ticketing systems

The NMS shall perform automatic correlation of the alarms associated with the same service in order to facilitate localization and source identification.

### **3.2 CONFIGURATION MANAGEMENT**

The NMS solution shall control and identify the elements of the telecommunications network, collect data from these elements, and provide them with data. To speed up the delivery of network services, the configuration management shall contain powerful tools that require few human interventions.

The NMS will be able to configure every electronic and optical device on the network and provision new services. Software revisions, configuration files, and data logs shall be able to be downloaded and uploaded. The NMS shall also be able to turn on or off remote devices. The NMS will validate untested configurations and store them in an easily retrievable format.

The NMS shall automatically back-up all network resource configurations on a timely basis.

Configuration management shall include the ability to keep track of configuration changes, either locally or remotely, and assign the changes to a specific network administrator.

### **3.3 ADMINISTRATION MANAGEMENT**

To prepare for future expansion and scaling, the NMS shall provide accounting functions to measure usage of individual telecommunications network resources. In addition, it shall provide inventory management, auditing and reconciliation of inventory data per NERC CIP.

The NMS shall administer a set of authorized users by establishing user credentials, passwords, and permissions.

The NMS shall provide backups and synchronize with the corresponding database.

### **3.4 PERFORMANCE MANAGEMENT**

The NMS shall assess the behavior and efficiency of network elements by tracking key performance indicators, particularly those enabled with SNMP. These include routers, switches and optical devices etc. The indicators shall include, but are not limited to, throughput, bandwidth utilization, response time, packet loss, latency, error rate, availability, uptime, and downtime. The NMS should also provide consistency and reliability metrics.

The NMS shall be capable of network performance analysis and improving management log quality by automating the creation of simple reports, charts, and graphs.

The NMS shall assist network administrators to carry out a performance measurement phase, to:

- Collect statistical data including traffic, blocking rate and quality of service from any points of interest in the network
- \*Analyze statistical data to improve the efficiency of the network
- \*Evaluate service availability through all network layers
- Facilitate planning, commissioning, maintenance and quality measurement
- \*Meet service-level agreements and service-level objectives
- \*Monitor various aspects of performance so that the network meets service-level agreements and service-level objectives

Performance information gathered by the NMS will alert network administrators when performance deviates from predefined thresholds.

Reporting tools shall provide the following functionalities:

- Reporting format templates
- Tailored reports preferably through a GUI type interface
- Exportation of report data in a commonly used format (Excel, CSL...)

### **3.5 SECURITY MANAGEMENT**

The NMS shall provide security for the network, the WAN, and all management functional areas. Security management includes network authentication, authorization and auditing, communications, and event detection and reporting.

The NMS shall control access to elements of the network by authentication, authorization, and encryption.

In particular, the NMS shall address functional safety management needs, namely:

- User access restrictions to network elements and resources
- Centralized management of user accounts and access privileges
- Encryption of sessions
- Session logging
- Administrator access
- Access control
- Secure access by use of encryption and authentication

The NMS shall offer classes of services to limit access rights to different users. It shall be impossible to escalate privileges without administrator's approval.

The NMS should support higher means of identification such as secure access devices, namely RSA SecurID, one-time password or biometrics.

### **3.6 NETWORK DEVICE DISCOVERY**

The NMS shall be capable of automatically identifying what devices are present on the network. New devices shall be discovered and reported. Unknown or intruder devices shall trigger an alert. The discovery mechanism shall be outlined for each network resource type.

### **3.7 NOTIFICATIONS**

Alerts will be able to be generated from the NMS. This involves configuring time-of-day with the on-call network administrators and pertinent competencies based on the nature of the fault. Alerts shall be provided by calling, texting, emailing, etc.

A list of supported SMS based integration tools such as Websphere MQ, Tomcat, Weblogic etc. shall be provided.

### **3.8 DATA LOGGING**

\*The NMS shall provide fault logs and compile statistics to determine the service level of individual network elements. They will be used to determine weak devices in the telecommunications network that require attention.

All configuration changes shall be logged, including hardware and software updates. Unauthorized or faulty configuration changes shall be flagged and an alert shall be provided to the network administrators.

Security-related information shall be gathered and analyzed regularly by the NMS. These include network attacks, intrusions and attacks on the NMS itself.

### **3.9 OPERATION, ADMINISTRATION AND MAINTENANCE**

The NMS shall provide a suite of diagnostic tools to enable the network administrator to validate and correlate network performance with service-level agreements.

### **3.10 OSS AND BSS INTEGRATION**

The NMS shall provide open interfaces to enable integration with third party OSS and BSS platforms.

Additional interfaces shall allow integration with a web portal. A list of supported interfaces and integration requirements will be provided.

An open interface shall provide full access to the NMS functionalities and network data.

Network faults, configuration mistakes and other events shall trigger notifications to the OSS.

### **3.11 SERVICE PORTAL**

The NMS shall include a web based user interface to control the configuration and the provisioning of services. The basic functions of the service portal shall include, without being limited to, the following:

- User profile access to NMS functions
- Fault detection and correction
- Reports on network performance and equipment status
- Asset inventory and tracking in accordance to NERC CIP
- Modification, addition, and deletion of work orders
- Configuration of all network elements
- Pre-existing or tailored reports on all portal parameters
- Network element troubleshooting with priorities and drill-down views
- Means to export reports into various office applications, servers, and services

The service portal shall be accessible from a wide range of computer and mobile platforms.

### **3.12 TROUBLE-SHOOTING**

The NMS shall collect key performance indicators concerning the network. The NMS shall provide advanced analytics that shall assist network administrators in rapidly troubleshooting problems.

The NMS shall monitor the integrity of signaling protocols such as IGP, BGP, OSPF, IS-IS, IP/MPLS, etc.

The NMS shall either configure or use pre-defined threshold parameters for fault-detection purposes.

### **3.13 HIGH AVAILABILITY**

The NMS hardware and software tools shall consist of a main station mirrored remotely on a hot standby station, and a stand-by station. They shall reside in three areas, namely:

- The main NMC with data center
- A hot standby NMC with data center
- A remote data center

It shall be possible at any time to changeover, either automatically or manually, from one NMS platform to a hot standby failover platform. The NMS shall also be accessible by a remote console from any point in the telecommunications network using SSH client application, or by other secure means.

## **4 MULTI-VENDOR ARCHITECTURE**

AVANGRID has a multi-vendor strategy in its telecommunication networks. Therefore, it is instrumental that proposed equipment complies with the standards. Any proprietary feature must be thoroughly explained, and its added value, justified.



## 4.1 INTEROPERABILITY

The equipment should have the ability to interface over standard MPLS interfaces.

Also, the integration must take into account that the network has to be managed in the most efficient way, in terms of service implementation, troubleshooting or incidents management.

The following aspects should be covered:

- a. Recommendation for network development in multi-vendor implementations. It is expected that the recommendation explains how to best achieve interoperability in different use cases: i.e.: multi-vendor Core Network or parallel Core Networks per each vendor, multiple vendors on the access part, etc.
- b. Detailed description for specific use cases, along with their configuration setups.

Interoperability information has to be provided, specifying the functionalities in which compatibility is achieved depending on the counterpart vendor.

As part of the procurement process a batch of testing shall be carried out in order to guarantee interoperability:

- Physical interfaces
  - IEEE802.1Q encapsulation
  - Qin1Q encapsulation
  - MTU: jumbo frames
  - Link Aggregation (LACP)
- Control Plane
  - OSPF Routing
    - P2P Neighbor
    - Single Area
    - OSPF DB
  - BGPv4 Routing
    - Neighbors
    - Routes
    - MP-BGP family inet-vpn
    - Authentication
    - Route Reflector
  - LDP
    - Neighbors
    - Database
    - LDP over RSVP
  - RSVP-TE
    - LSPs
    - Secondary no pre-sigaled
    - Secondary pre-sigaled
    - Primary/secondary switchover
    - Strict/loose paths
    - Primary and secondary path EROs with no common points and CSPF 140
    - Primary and secondary path EROs with common points and CSPF 140
    - Primary and secondary path EROs with common points and CSPF .141

- QoS
  - Ingress QoS
  - Egress QoS
  - Classification
    - BA Classification
      - IP BA Classification
      - MPLS BA Classification
    - Multifield Classification
      - Classification IP BA
- Rewrite
  - Ingress IP – Egress Rewrite IP
  - Ingress IP – Egress Rewrite MPLS+IP
  - Ingress MPLS – Rewrite IP
  - Ingress MPLS – Rewrite MPLS
- Queuing
- Congestion
  - Scheduling
  - High-priority level
  - Per VLAN scheduling
  - WRED
  - Traffic shaping
  - Policers
  - Ingress scheduling
- Services
  - L3VPN
    - Routing PE-CE (static, bgp, OSPF)
    - VRF Export/import policies
    - Communities: add/delete
  - L2VPN-VPLS
    - Access Ethernet
      - Flexible vlan-tagging
      - Flexible Ethernet Services
    - Pseudowire Stitching
      - Stitching within VPLS instance
    - VPLS – FEC128
      - Maintaining VLAN tags from packets sent
      - Removing VLAN tags from packets sent
- Management
  - Management protocols
    - Tenet Access
    - SSH Access
    - FTP Access
    - Syslog
    - SNMPv3

- Get
- Trap
- Radius
- LDAP
- FF protect RE
- Ingress
- Vendor's management system capable of detecting nodes from other vendors (or gathering information once registered by hand on the system)
- Solarwinds integration
- SDN support for third parties SDN platforms (Netconf, Yang Diagrams)

Interoperability must be tested and proven within our current lab environment for the hardware and software. If interoperability is not demonstrated, vendor may be disqualified.

## 4.2 MANAGEMENT

The equipment should have the ability to be managed by third party management software using standard protocols as SNMPv3.

Each vendor shall indicate their compliance degree with NETCONF and YANG.

### 4.2.1 UMBRELLA SYSTEM

The NMS shall be compatible with the umbrella system being deployed in the NMC which is Solarwinds.

## 5 CYBERSECURITY

Key elements of the strategy are:

- NERC CIP Version 5
- IEC 62351 Power Systems Management and Associated Information Exchange — Data and communications security
- ITU-T X.805

The key security requirements are listed below:

- Authentication/Authorization/Accounting (AAA)
- Local
- RADIUS
- TACACS+
- Access Filters
- \*\*Network Address Translation (NAT)
- \*\*Zone-based Firewall
- Encryption
- \*\*IP Sec
- .
- VPRN
- VPLS
- VLL (TDM, IP, Ethernet, Frame Relay, HDLC)

- Event logging
- MD5 authentication (OSPF, RSVP-TE)
- SSH
- SNMPv3
- 802.1x authentication
- Access control (log-in control, strong password)
- SFTP (IPv4/IPv6)

## **6 CONTINUOUS DIAGNOSTICS AND MITIGATION (CDM)**

The successful vendor will support all aspects of Security Operations Center (SOC) service delivery and will work across all stakeholders as necessary to provide acceptable assurance to Avangrid Security.

Stakeholders include but are not limited to:

- Business owners
- Technical custodians
- Data custodians
- Performance Assurance and Management
- Security metrics and reporting

The successful vendor will be responsible to provide tools, techniques, procedures, and professional support necessary to achieve the objectives of the Avangrid Security Operations Center (SOC).

Security Operations Capability Objectives include but are not limited to:

- Manage Hardware Assets
- Manage Software Assets
- Manage Configuration Settings (CCEs)
- Manage Vulnerabilities
- Manage Boundaries - Physical
- Manage Boundaries - Encryption
- Manage Boundaries - Filters - Network Packet, Network Layer 2, Network Access Protection, Encapsulation, Content, Data Leaks/Loss Prevention
- Manage Trust in People Granted Access
- Manage Security Related Behavior
- Manage Credentials & Authentication
- Manage Privileges and Accounts
- Prepare for Incidents and Contingencies
- Detect Suspicious Events / Patterns
- Respond to Incidents and Contingencies
- Manage Requirements, Policy, and Planning
- Manage Security Quality - Reliability, Availability, Maintainability
- Manage Risk
- Manage Cost including Opinion of Cost analysis and Investment Analysis

Vendor will work with Avangrid to integrate with Security measures and COTS (Common off the Shelf) technologies.

Avangrid is modeling, adapting, and adopting a Continuous Diagnostics & Mitigation program (CDM). Please see the attached links for further context:

- <https://www.dhs.gov/cdm>
- <https://www.us-cert.gov/cdm/home>
- <https://www.gao.gov/assets/700/691439.pdf>

## **7 STANDARDS COMPLIANCE**

The DWDM system shall be tested to meet NEBS Level 3 certification. Vendor shall provide information detailing the level of design, testing and compliance certification achieved. The system shall also be RoHS compliant. The system shall comply with the following:

- UL/CSA 60950-1, ITU-T G.664 (10/2012) Amd.1 (12/2014) and FIPS 140-2.
- IEEE Std. 1613-2009 - Environmental and Testing Requirements for Communications Networking Devices Installed in Electric Power Substations.
- IEC 61850-3:2013 and IEC IEC 61000-6-5:2015,
- IEEE 1613, specification for communications networking devices in electric power substations.
- ANSI/IEEE C37.90.2, specification for Radio Frequency Interference (RFI).
- ANSI/IEEE C37.90.1, specification for electrical isolation.
- Telcordia TR-NWT-000332, specification for equipment reliability.

If the equipment is TL-9000 certified, a certificate shall accompany the equipment specification. Any other relevant certification shall be included.

TL9000: <https://www.juniper.net/assets/us/en/local/pdf/certificates/juniper-networks-tl-9000.pdf>

- NEBS: [https://www.juniper.net/documentation/en\\_US/release-independent/junos/topics/reference/agency-approvals/mx240.html](https://www.juniper.net/documentation/en_US/release-independent/junos/topics/reference/agency-approvals/mx240.html)
- MX104 Agency Approvals and Compliance:  
[https://www.juniper.net/documentation/en\\_US/release-independent/junos/topics/reference/agency-approvals/mx104-agency-approvals.html](https://www.juniper.net/documentation/en_US/release-independent/junos/topics/reference/agency-approvals/mx104-agency-approvals.html)
- MX960 Agency Approvals and Compliance:  
[https://www.juniper.net/documentation/en\\_US/release-independent/junos/topics/reference/agency-approvals/mx960.html](https://www.juniper.net/documentation/en_US/release-independent/junos/topics/reference/agency-approvals/mx960.html)
- MX10003 Agency Approvals and Compliance:  
[https://www.juniper.net/documentation/en\\_US/release-independent/junos/topics/reference/agency-approvals/mx10003-agency-approvals.html](https://www.juniper.net/documentation/en_US/release-independent/junos/topics/reference/agency-approvals/mx10003-agency-approvals.html)

## **8 ECONOMIC AND COMMERCIAL CONDITIONS**

Prices will be delivered itemized by chassis, card and interface.

Maintenance will be quoted on the basis that AVANGRID has a group of technicians trained and qualified to solve most of the incidents. Expert support will be quoted.

Prices are fixed and not subject to revision.

## **9 AFTER-SALES SERVICE**

Vendors shall indicate the means they have for after-sales assistance, listing average repair and replacement times. See ANNEX I

Juniper Networks Technical Assistance Center (JTAC) is available 24 hours a day, 7 days a week and 365 days of the year. Juniper maintains multiple TAC centers across an international geography to ensure our customers have access to the support they need at all times. The escalation timeframes are determined by the priority level – critical, high, medium and low. For a critical case either the VP of Customer Service or VP of Engineering and Sales will be involved by the 4 hour mark. For more information on JTAC please refer to the following links:

- [Contact Support](#)
- [JTAC User Guide](#)
- [JTAC Fact Sheet](#)

### **9.1 MAINTENANCE AND REPAIR SERVICE**

The vendor will provide a complete proposal for this service, customized for AVANGRID. Duration of the service will be one year.

### **9.2 SOFTWARE UPDATES**

The vendor will inform AVANGRID about new software versions and the improvements they provide for system operation (release notes).

The necessary software updates will be offered for the correct functioning of the systems, or for the use of new equipment or services.

Junos software updates are available for download on the Juniper support website, contingent upon maintaining an active annual JCare support contract. Junos releases are backward compatible with prior Junos releases. Migration strategies can be incorporated as a part of the Professional Services engagement.

During the term of the Juniper Networks Service Contract, Juniper Networks shall make available the Supported Updates (as defined below) to End User solely for support of the End User's Supported Juniper Product, subject to the terms and conditions set forth below:

- Rights in Supported Updates. For each Supported Update with regard to the Software (as defined in the End User License Agreement or EULA) originally embedded in, delivered with, or consisting of the End User's Supported Juniper Product, the End User's rights in any such Supported Update will be subject to:
  - The terms of the EULA
  - Any applicable Entitlement (as defined in the EULA) with respect to the original Software
  - Those same restrictions and conditions that apply to the original Software

- Definitions.

(1) As used herein, "Supported Updates" (or "Supported Release") as of a particular time means any Update (as defined in the EULA) of the Software consisting of or then available generally to End Users of the Juniper Networks product, provided, however, that Supported Update excludes:

- Any Chargeable Releases (defined below) (and any other Updates based on any such Chargeable Release) that are made available after the original Software licensed to the End User, unless End User has separately purchased a license to such Chargeable Release, and such Chargeable Release is itself Juniper Networks product
- Any Separately Licensable Feature (as defined in the EULA) embedded in or otherwise associated with the Software (and any Updates of any such Separately Licensable Feature), unless End User has separately purchased a license to such Separately Licensable Feature, and such Separately Licensable Feature is itself a Supported Juniper Product
- Any Update that is no longer eligible for support under applicable Juniper Networks standard End-of-Life/End-of Support policies

Note that availability of such release at any particular time is subject to then current software End-of-Life and End-of-Support policies posted at <https://www.juniper.net/support/eol/990833.pdf>

(2) "Chargeable Release" means a release of Software that, due to its enhancements in functionality or performance from prior releases, is made available by Juniper Networks only upon payment Under the Juniper Care Support Offering, AVANGRID would have access to a portal that provides this type of information. Email notifications can be set by the customers.

## **10 TRAINING**

The vendor shall offer a training course (repeated in two sessions) for AVANGRID staff, which covers the necessary know-how for the operation, management and administration of the network and its management system. Flexibility is required to adapt training to staff schedule and shifts.

## **11 WARRANTY**

The warranty of the equipment will be two years from acceptance by Avangrid. Optionally a 5 year warranty extension period shall be priced (for a total of 7 years warranty).

The vendor will provide a basic list of spare parts with prices, for repair by AVANGRID O&M team, as well as repair rates by the vendor itself.

Vendor shall guarantee availability of spare parts for the equipment for a minimum period of 5 years.

Juniper Networks offers extended warranties with advanced replacement, Juniper Care Service contract to cover beyond the first year standard warranty. For information on our standard warranty policies please refer to the links below.

- [Product Warranty Policy](#)
- [Software Product Warranty Matrix](#)

## **12 PACKAGING**

The packaging of the equipment will be adequate to allow long-term storage in a warehouse. The packaging for each device will clearly identify vendor, model and serial number.



## ANNEX I

The following describes the after-sales services, maintenance and technical support that must be supplied by the bidders for the requested equipment.

### TECHNICAL SUPPORT SERVICE

The Technical Support service of 2nd and 3rd tier must be provided by a high level Technical Assistance group and knowledge of the equipment offered. This service must include the attention, diagnosis, neutralization and solution, remotely, of those incidents that, due to their difficulty, exceed the capabilities of the AVANGRID's 1st Level staff.

This service must be available 24 hours a day, 7 days a week, and must be attended by technicians to whom the incident is assigned, so that technical support must be provided from the group of specific support for these teams that the bidder considers.

The following benefits must be included:

- **Diagnosis, neutralization and resolution of incidents:**

Intervention must be made, at the express request of AVANGRID, when the 1st Level maintenance staff has exhausted all their technical resources to resolve the anomaly

In the event of an incident, the first analysis of the situation may be made through a remote connection via VPN to the management platform of the equipment; after this analysis, the appropriate corrective actions that may be carried out directly through the platform or, when they require manipulation of the HW, with the on-site support of AVANGRID's top-level personnel will be proposed.

The technical management, during the resolution of the incidents, will be in the hands of the technical staff that provides the support that will propose the corrective measures and will ask AVANGRID for the permits and action windows to be able to execute them.

In case of hardware problems, according to the agreed replacement method the maintainer must perform the reinstallation of the service

The maintainer will be ultimately responsible for leaving the system in the state prior to the fault once the HW problem has been solved.

The provider must provide a quarterly report of the incidents or queries attended, as well as the status of the review of the backups made, if any.

- **Product Support Engineering:**

The support must have a Product Support Engineering, so that if necessary, any reported technical incidence can be escalated to that department

- **Software Upgrades**

Software Upgrade comprise the New Generic where new features or new features are included) and software upgrades (generic product level). In essence Software Upgrades must consist of versions that contain new features and functionalities, which are normally

provided in data carriers, not being downloaded from an electronic interface the New Generics.

- **Telephone attention to inquiries**

Telephone attention about technical queries, related to the equipment described in this document and that are not caused by anomalies in its operation, from 9:00 a.m. to 5:30 p.m. during working days.

Telephone attention to technical queries, related to the equipment described in this document and caused by anomalies in its operation. The hours of service must be permanent for 24 hours a day, every day of the year.

## **SEVERITY LEVELS**

The severity of an incident shall be established by AVANGRID at the time of requesting assistance, according to the definitions in the following sections. These severity levels may be modified by AVANGRID, by phone call or by e-mail, depending on the evolution of the incident and its impact on the network or management systems.

- **Critical**

They will be considered of a Critical severity those actions which lead to serious traffic losses, cause serious communication interruptions or traffic cuts in preferred customers.

- **Major**

They will be considered "High severity" those actions that lead to the isolation of installations or acute traffic lose.

- **Minor**

Those actions taken with the aim of resolving failures without affecting the service or that do not affect its correct operation will be considered as actions with a lower priority level.

In cases where the solution provided is not definitive but provisional, once restored the affected service, it will get a lower priority defined according to the new severity of the problem and therefore will have a resolution time according to the previous definitions.

After the resolution of an incident, a report must be issued detailing the cause and actions taken to recover the service.

## **SERVICE LEVELS**

To describe the service levels of the technical support described in this Annex, the following parameters are defined:

- Service window: Time zone in which this service should be offered
- Response time: Time elapsed between the reception of the fault by the 2nd level of the support and the first call of the technicians to the staff of AVANGRID

- Neutralization time: Time elapsed since the opening of a service incident and remote neutralization by means of a temporary or definitive solution that allows the restoration of the affected service

Thus, the Technical Assistance service of support for incidents must meet the following levels of service:

	<b>CRITICAL</b>	<b>MAJOR</b>	<b>MINOR</b>
<b>Service Window</b>	<b>24 hours, all days of the year</b>	<b>24 hours, all days of the year</b>	<b>24 hours, all days of the year</b>
<b>Response Time</b>	30 Minutes	1 Hour	1 hour in working hours
<b>Neutralization time</b>	4 Hours	8 Hours	Agreed with the client

For the attention to telephone consultations, the following levels of service are established:

	<b>Caused by plant anomalies</b>	<b>Not-Caused by plant anomalies</b>
<b>Service Window</b>	24 hours, all days of the year	Working days, from 9:00 am to 17:30pm
<b>Response Time</b>	1 Hour	4 Hours
<b>Neutralization Time</b>	As per Service Levels	Agreed with the client

Understanding, in this case, as time of neutralization the time elapsed until providing the information requested by AVANGRID.

Juniper Networks support is based on a foundation of our Juniper Care offering. At its core, Juniper Care is a maintenance contract for each device and/or software license. It provides 24x7x365 access to Juniper Networks Technical Assistance Center and award-winning self-service Customer Support Center, a variety of hardware replacement options based on geographic availability, and software releases.

### *Juniper Care Support Option Entitlements*

*Table 2 lists entitlements and hardware replacement choices for each Juniper Care support option.*

Table 1: Juniper Care Support Option Entitlements

<b>PRIMARY LEVEL OF SUPPORT</b>	<b>Juniper Care Core</b>	<b>Juniper Care Core Plus</b>	<b>Juniper Care Next-Day Ship</b>	<b>Juniper Care Next-Day Delivery</b>	<b>Juniper Care Next-Day Onsite</b>	<b>Juniper Care Same-Day Delivery</b>	<b>Juniper Care Same-Day Onsite</b>
Unlimited JTAC 24X7	X	X	X	X	X	X	X
Software releases	X	X	X	X	X	X	X
CSC online e-support	X	X	X	X	X	X	X
Junos Space Service Now/Service Insight	X	X	X	X	X	X	X
E-learning	X	X	X	X	X	X	X
Return-to-factory		X					
Next-business-day advanced replacement parts shipment			X				
Next-business-day advanced replacement parts delivery				X	X		
Same-day advanced replacement parts delivery						X	X
Onsite technician					X		X

Next Day, Next Day Ship, and Same Day service level is subject to availability; please check Juniper service availability tool for coverage.

*For more details on Juniper Care features and entitlements, please refer to the following resources:*

[Juniper Care Service Description](#)

[Juniper Care Software Advantage Service Description](#)

[End User Support Agreement](#)

## **INFRASTRUCTURE**

The bidder to cover the support and maintenance of this equipment must have a permanent Management Center, twenty-four hours a day, every day of the year, which will be responsible for

receiving all AVANGRID service calls and will make them reach the corresponding technical staff, with enough haste to fulfill the commitments of the previous point.

The support service must have a system for recording and tracking incidents in which they will be consolidated as well as the corresponding status.

It must also have a computer with the possibility of remote connection, via VPN, authorized by AVANGRID S.A., which will allow interventions to be carried out more efficiently.

### **HARDWARE REPLACEMENT SERVICE AND REPAIR OPTION**

To complement the Technical Assistance and Maintenance service, the option of providing a repair and replacement hardware service from the equipment described in this document will be evaluated.

In the case of hardware replacement service, this consists of replacing the equipment in the event of a breakdown by equal or similar equipment with all the functionalities equipped with the damaged equipment. Includes "remote hands assistance", when necessary: presence of a technician on site to replace the damaged equipment and the configuration of the spare part so that AVANGRID can acquire its remote control.

The hours of attention and response times that are requested in these cases are in the 24x7x4 mode.

- Permanently 24 hours a day, 7 days a week
- Response time (RT) of less than 30 minutes measured in natural time

Repair service in case of detected defective equipment must contain all necessary tasks to repair these units:

- Single point of contact where AVANGRID will have to send the plates to be repaired
- Return Material Authorization Request (RMA)
- Reception of the damaged unit in a Logistics Repair Center
- Equipment repair
- Transportation to the premises indicated by AVANGRID
- Complete and continuous monitoring of the Unit to be repaired

Below are the Service Levels (SLAs) proposed in two modes "repair and return" and "advanced repair service":

<b><i>SERVICE LEVEL</i></b>	<b>REPAIR AND RETURN</b>
Reception availability and material to be repaired	8X5
Repair Time	60 days
Force Majeure Time	To Discount

- In those cases in which the time established for reasons of force majeure is exceeded, it will be deducted from the global calculation of the REPAIR of delay times.
- The repair times will be determined basically by the time elapsed between the reception to the single window of maintenance repairs, the repair time in the workshops and the delivery to the AVANGRID premises.

Juniper Networks support is based on a foundation of our Juniper Care offering. At its core, Juniper Care is a maintenance contract for each device and/or software license. It provides 24x7x365 access to Juniper Networks Technical Assistance Center and award-winning self-service Customer Support Center, a variety of hardware replacement options based on geographic availability, and software releases.

### *Juniper Care Support Option Entitlements*

*Table 2 lists entitlements and hardware replacement choices for each Juniper Care support option. Table 2: Juniper Care Support Option Entitlements*

<b>PRIMARY LEVEL OF SUPPORT</b>	<b>Juniper Care Core</b>	<b>Juniper Care Core Plus</b>	<b>Juniper Care Next-Day Ship</b>	<b>Juniper Care Next-Day Delivery</b>	<b>Juniper Care Next-Day Onsite</b>	<b>Juniper Care Same-Day Delivery</b>	<b>Juniper Care Same-Day Onsite</b>
Unlimited JTAC 24X7	X	X	X	X	X	X	X
Software releases	X	X	X	X	X	X	X
CSC online e-support	X	X	X	X	X	X	X
Junos Space Service Now/Service Insight	X	X	X	X	X	X	X
E-learning	X	X	X	X	X	X	X
Return-to-factory		X					
Next-business-day advanced replacement parts shipment			X				
Next-business-day advanced replacement parts delivery				X	X		
Same-day advanced replacement parts delivery						X	X

PRIMARY LEVEL OF SUPPORT	Juniper Care Core	Juniper Care Core Plus	Juniper Care Next-Day Ship	Juniper Care Next-Day Delivery	Juniper Care Next-Day Onsite	Juniper Care Same-Day Delivery	Juniper Care Same-Day Onsite
Onsite technician					X		X

Next Day, Next Day Ship, and Same Day service level is subject to availability; please check Juniper service availability tool for coverage.

*For more details on Juniper Care features and entitlements, please refer to the following resources:*

[Juniper Care Service Description](#)

[Juniper Care Software Advantage Service Description](#)

[End User Support Agreement](#)

After the repair, a report must be issued with the description of the cause of the failure, as well as details of the repair.

### **Liquidated Damages**

Quarterly an analysis of the interventions made during that period will be made, while for the revision of the repairs the time will be one year.

If the number of interventions in which the neutralization time is not honored is greater than 5% of the total number of interventions, AVANGRID may apply Liquidated Damages according to the following scheme:

- No. Interventions with SLA (neutralization time) unfulfilled between 5% and 10% of the total of interventions, the Liquidated Damages will be 2% of the billing corresponding to three months
- Number of non-complied SLA interventions between 10% and 15% of the total of interventions, the Liquidated Damages will be of 5.5% of the billing corresponding to three months
- Number of unfulfilled SLA interventions between 15% and 20% of the total of interventions, the Liquidated Damages will be 10% of the billing corresponding to three months

Regarding the number of repairs in which the return time is not observed is greater than 10% of the total shipment, AVANGRID may apply Liquidated Damages according to the following scheme:

- Number of unfulfilled returns between 10% and 15% of total shipments, the Liquidated Damages will be 2% of the billing for three months
- Number of unfulfilled returns between 15% and 20% of total shipments, the Liquidated Damages will be 5.5% one of the billing for three months
- Number of unfulfilled returns greater than 20% of total shipments, the Liquidated Damages will be 10% of the billing for three months

Juniper recommends JCARE, JCARE Plus Service Manager and Optimum Care with Advanced Service Engineering Credits so that Service Levels are consistent and meet AVANGRID's

expectations. Juniper also recommends better alternatives to the mentioned return to factory or repair service, such Juniper JCARE advanced replacement service available as Same or Next Business Day. A customer sparing program is also an option. These services are better suited to meet service levels on an on-going basis. While Liquidated Damages are understood to be a request for enforcement in contract, Juniper proposes proven methods for mutual success that help prevent issues during the lifecycle of problem resolution such as JCARE Plus and Optimum Care. JCARE Plus and Optimum Care are specifically designed to increase the success of meeting SLAs and remedy issues.

Juniper Care Plus empowers organizations to meet today's challenges by delivering proactive personalized services designed to maximize application reliability and avoid incidents. This helps ensure that your network is always at optimum readiness, able to evolve smoothly and effectively in response to the demands of your organization's goals. Juniper Care Plus provides enhancements over and above a standard support contract. Juniper Care Plus keeps the network at optimum readiness through high touch support (service manager), and personalized services such as training, network consulting, and account management—all mitigating risk for organizations, providing application reliability, reducing the learning curve, and accelerating time to value.

A primary benefit of Juniper Care Plus is the Juniper Service Manager—your advocate within Juniper Networks to manage all service-related operational activities during local business hours. The Juniper Service Manager is a named contact and your advocate within Juniper to manage all service-related activities during local business hours. Your Service Manager is the single point of contact within Juniper to oversee the delivery of all entitled services in the Juniper Care Plus offering.

The Service Manager's responsibilities include:

- Formulate and deliver a Service Support Plan
- Provide account setup assistance and ongoing account management to ensure that you have access to service deliverables in the Juniper Care Plus offering and
- appropriate resources within Juniper
- Manage customer escalation related to service support, service readiness, and service planning, working with Juniper internal delivery teams
- Conduct periodic conference calls to report status on outstanding issues and discuss key future network activities
- Conduct quarterly operational review meetings to discuss your specific product and service performance, metrics, related trends, and planned services activities
- Provide case trend analysis that includes a regular review of your reports to identify repeat tactical hardware, software, or operational issues
- Provide logistic and operational assistance
- Provide proactive case planning

For more information, please see our Juniper Care Plus Service Description.

<https://www.juniper.net/us/en/local/pdf/datasheets/1000324-en.pdf>





**SCHEDULE C****Terms and Conditions****TABLE OF CONTENTS**

<b><u>Agreement Article - Description</u></b>	<b><u>Page</u></b>
COMPANIES.....	9
ARTICLE 1 – CONTRACT DOCUMENTATION.....	44
ARTICLE 2 – ALTERATION OF TERMS.....	44
ARTICLE 3 – COMPLIANCE WITH LAWS AND INDEMNIFICATION.....	44
ARTICLE 4 – DRAWINGS, DESIGN, DATA, CREATIVE WORK AND INVENTIONS.....	45
ARTICLE 5 - CHANGES.....	45
ARTICLE 6 - WAIVER.....	46
ARTICLE 7 – DELIVERY; SCHEDULE; DELAYS .....	46
ARTICLE 8 – CONTRACT PRICE.....	47
ARTICLE 9 – PAYMENT .....	47
ARTICLE 10 – DELEGATIONS; SUBCONTRACTS; ASSIGNMENT .....	48
ARTICLE 11 – SET-OFF .....	48
ARTICLE 12 - INSPECTION.....	48
ARTICLE 13 - WARRANTY.....	49
ARTICLE 14 – SAFETY .....	49
ARTICLE 15 – PATENTS AND OTHER INTELLECTUAL PROPERTY; INDEMNIFICATION .....	49
ARTICLE 16 – TERMINATION FOR CAUSE.....	50
ARTICLE 17 – TERMINATION FOR CONVENIENCE .....	51
ARTICLE 18 – INSURANCE AND GENERAL INDEMNIFICATION .....	51
ARTICLE 19 – FORCE MAJEURE .....	52
ARTICLE 20 - SUBSTITUTION.....	53
ARTICLE 21 – INDEPENDENT CONTRACTOR .....	53
ARTICLE 22 – AUDIT RIGHTS.....	53
ARTICLE 23 - LIENS.....	53
ARTICLE 24 - TAXES .....	54
ARTICLE 25 – SPARE PARTS.....	55
ARTICLE 26 - SEVERABILITY.....	55
ARTICLE 27 – COMPLETE AGREEMENT .....	55
ARTICLE 28 - CONFIDENTIALITY.....	55
ARTICLE 29 - TITLE .....	56

**ARTICLE 30 - PUBLICITY.....56**  
**ARTICLE 31 – GOVERNING LAW.....56**  
**ARTICLE 32 – EMPLOYEE SOLICITATION.....56**  
**ARTICLE 33 – ETHICS.....57**  
**ARTICLE 34 – NO DISPUTE.....57**  
**ARTICLE 35 – SECURITY REQUIREMENTS.....57**  
**ARTICLE 36 – CONTINUOUS IMPROVEMENT .....59**  
**ARTICLE 37 - UTILIZATION OF SMALL BUSINESS CONCERN.....59**  
**ARTICLE 38 - SMALL BUSINESS SUBCONTRACTING PLAN.....59**  
**ARTICLE 39 - SURVIVAL.....59**

## **ARTICLE 1 – CONTRACT DOCUMENTATION**

Pursuant to that certain Master Materials Procurement Agreement (the “Agreement”) between Avangrid Service Company (hereinafter, “Customer”), and [REDACTED] [REDACTED] (hereinafter, “Supplier” or “Vendor”), the entity (Customer and/or Company(ies)) named in the given Purchase Order and SOW, engages the Supplier, and the Supplier hereby agrees to provide the Materials.

The Materials shall be as described in *Schedule B* of the Agreement, as such Schedule may be amended, modified or supplemented and attached hereto for the purposes of the Purchase Order.

The provision of the Materials shall be governed by the order of precedence set forth in the Agreement, Section 2.2(c) of the Agreement.

All Material shall be invoiced in accordance with the pricing schedule approved by Customer, “Pricing Schedule,” included in *Schedule D*, attached hereto and made a part hereof (unless otherwise agreed to in writing by the Company or Customer).

## **ARTICLE 2 – ALTERATION OF TERMS**

None of the terms and conditions contained in this Agreement may be waived, altered, modified, or added to unless such waiver, alteration, modification or addition is in writing and signed by an authorized representative of the Company and Supplier. Except as set forth in the previous sentence, each shipment from Supplier to the Company shall be only upon the terms and conditions set forth in this Agreement, notwithstanding any terms and conditions that may be contained in any acknowledgment, invoice, or other form of Supplier, and notwithstanding the Company’s act of accepting or paying for any shipment or any similar act of the Company.

## **ARTICLE 3 – COMPLIANCE WITH LAWS AND INDEMNIFICATION**

A. Supplier warrants that it will comply with all applicable federal, state and local laws, statutes, ordinances, rules, regulations and executive orders of each applicable governmental entity, board and/or agency, and that it will defend, indemnify and hold harmless, to the fullest extent permissible by law, the Company from and against any and all liabilities, claims, costs, expenses, losses and judgments arising from Supplier's failure to so comply.

B. Supplier shall comply to the extent applicable, with Executive Order 11246, the Vietnam Era Veterans Readjustment Assistance Act of 1974, the Rehabilitation Act of 1973, as amended, and its or their implementing regulations, and reporting requirements there under. The Equal Opportunity and Affirmative Action clauses contained in Title 41, Chapter 60, Sections 1.4, 250.4, and 741.3 of the Regulations of the U.S. Department of Labor, Office of Federal Contract Compliance, and any section or sections superseding or amending the same, are hereby incorporated herein by reference and made a part hereof as though fully set forth where applicable.

Without limiting the foregoing, the Supplier and each of its subcontractors (if any) shall abide by the requirements of 41 CFR 60-1.4(a), 60-300.5(a) and 60-741.5(a). These regulations prohibit discrimination against qualified individuals based on their status as protected veterans or individuals

with disabilities, and prohibit discrimination against all individuals based on their race, color, religion, sex, sexual orientation, gender identity or national origin. Moreover, these regulations require that covered prime contractors and subcontractors take affirmative action to employ and advance in employment individuals without regard to race, color, religion, sex, sexual orientation, gender identity, national origin, disability or veteran status.

#### **ARTICLE 4 – DRAWINGS, DESIGN, DATA, CREATIVE WORK AND INVENTIONS**

All drawings, sketches, designs, design data, specifications, notebooks, technical and scientific data, photographs, negatives, reports, findings, recommendations, data, information, memoranda, materials, creative works, inventions, innovations and other work products of every description relating thereto, as well as all copies or descriptions of the foregoing, prepared, created or completed by Supplier and paid for by the Company, pursuant to this Agreement (the “Work Product”), shall be subject to inspection by the Company at all reasonable times (for which inspection of the proper facilities shall be afforded the Company by the Supplier), shall be deemed to have been created or prepared by the Supplier for the Company on a work-made-for-hire basis, shall be the property of the Company and may be used by its employees or agents, or its subcontractors or vendors, and shall be delivered to the Company, or otherwise disposed of by the Supplier, either as the Company may from time to time direct or in any event as the Company shall direct upon completion or termination of this Agreement. To the extent any of the foregoing are not deemed a work for hire by operation of law, Supplier hereby irrevocably assigns, transfers, and conveys to the Company without further consideration all of its right, title, and interest in such Work Product, including all rights of patent, copyright, trade secret or other proprietary rights in such materials.

The Work Product, and all other information provided hereunder shall be treated by the Supplier as strictly confidential, and shall not be disclosed, copied, or used on behalf of any third party without the prior written consent of the Company.

Notwithstanding the foregoing, but expressly excluding the Work Product, Company acknowledges that Supplier exclusively owns and retains all of its own pre-existing intellectual property and proprietary rights existing prior to the Effective Date, including but not limited to Supplier’s proprietary software and tools, report templates, schematics, procedures, databases, methods, manuals, know-how, copyrights, trade secrets, trademarks, and any other proprietary rights to Supplier’s own software and materials (“Supplier’s IP”). To the extent that any of Supplier’s IP is reasonably necessary for Company, Customer and/or its contractors to exercise its rights in the Work Product, Supplier grants Company, Customer and their contractors a non-exclusive, worldwide, perpetual, royalty-free right-to-use license, without the right to sublicense, for the purposes intended under this Agreement or any SOW.

#### **ARTICLE 5 - CHANGES**

A. The Company shall have the right to make changes in the drawings or specifications. No changes shall be made except under the written order of a contract amendment submitted by the Company or Customer under the Agreement.

B. If Supplier claims that any instructions by drawings, specifications or otherwise approved or issued by the Company after the date of the Agreement involve extra cost or time for performance under this

Agreement, the Supplier shall give written notice to the Company including an estimate of changed cost or time thereof within ten (10) days after the receipt of such instructions, and in any event before proceeding to execute the work, unless otherwise directed by the Company, or except in an emergency endangering life or property. No such claim for additional compensation or time shall be considered unless so made. If the change as ordered by the Company increases or decreases the cost of the material or equipment to be supplied, or time for performance established in the Agreement, a fair and reasonable amount, as agreed upon by the Company and Supplier, shall be added to or subtracted from the compensation or completion date.

C. If, within ten (10) days after Supplier has provided an estimate of changed cost and/or time, the parties are unable to conclude a mutually satisfactory agreement, Supplier shall proceed with supplying the material or equipment as changed or modified until the differences are resolved. The parties shall endeavor to resolve any disputes regarding increases or decreases in costs resulting from such changes promptly through reasonable means, including, without limitation, impartial third party estimates or mediation.

#### **ARTICLE 6 - WAIVER**

No waiver by the Company, whether express or implied, of any of the terms or conditions of this Agreement, shall be or be construed to be a continuing waiver, nor deprive Company of the right to enforce or rely upon any such terms or conditions thereafter.

#### **ARTICLE 7 – DELIVERY; SCHEDULE; DELAYS**

“TIME IS OF THE ESSENCE” in the Supplier's performance of this Agreement. Deliveries are to be made according to the Company's terms as to time, quantities, and location, with the Company reserving the right to cancel, reject or refuse any delivery made prior to or subsequent to the times specified, if the quantities are not as specified, or if the delivery has been made to an improper location. If delivery as specified cannot be maintained, the Company must be notified immediately. Upon Supplier's failure to maintain delivery, the Company reserves the right to procure equivalent Material elsewhere, in whole or in part and to charge Supplier with any additional costs incurred.

Without prejudice to other remedies that Company may have under the Agreement or the law, if Supplier fails to meet the time schedule or other delivery date obligations set forth in the Agreement (the “Guaranteed Delivery Dates”), then Supplier shall pay to Company as liquidated damages for such delay, and not as a penalty, the amounts set forth in the applicable Agreement, if any, for each day the delivery is late under the applicable Agreement (the “Liquidated Damages”). If the Agreement does not establish an amount, the amount of the Liquidated Damages shall be equal to the amounts set forth in Schedule B of this Agreement.

The Parties acknowledge and agree that because of the unique nature of the performance it is difficult or impossible to determine with precision the amount of damages that would or might be incurred by Company as a result of Supplier's failure to meet the Guaranteed Delivery Dates under the applicable Agreement, Statement of Work, or applicable order. It is understood and agreed by the Parties that (i) Company shall be disadvantaged by failure of Supplier to meet such obligations, (ii) it would be impracticable or extremely difficult to quantify the amount of Company's damages resulting therefrom,

and (iii) any Liquidated Damages payable under the applicable Agreement, Statement of Work, or applicable order are not a penalty, but instead represent a fair and reasonable estimate of damages for failure to meet Supplier's Guaranteed Delivery Dates.

In no event shall the payment of any Liquidated Damages excuse Supplier from performance of any of its other obligations under this Agreement or prejudice Company's rights under the Agreement or Applicable Law.

Company shall have the right to deduct any Liquidated Damages due from the payment of any pending invoices to Supplier.

## **ARTICLE 8 – CONTRACT PRICE**

Supplier agrees that the prices (including, without limitation, the Contract Price) stated in this Agreement and on the face of each Purchase Order issued under this Agreement are firm unless otherwise noted on the face of the Purchase Order, and the Supplier warrants that said price(s) do not individually or in the aggregate exceed the prices allowed by any applicable federal, state or local law, regulation, or order.

## **ARTICLE 9 – PAYMENT**

A. Company shall either pay the invoice in accordance with payment terms agreed upon and stated in *Schedule D* attached to this Agreement and included in the purchase order, or withhold payment in accordance with Article 9(B) below.

B. Upon prior written approval and agreement from Supplier, Company may in certain situations withhold, or, on account of subsequently discovered evidence, nullify the whole or part of any disputed invoice to such extent as may be necessary to protect itself from loss. Such situations shall include, but not be limited to, discovery of:

- (a) defective Material;
- (b) third party claims filed or reasonable evidence indicating probable filing of such claims;
- (c) failure of the Supplier to make payments due to subcontractors, material Suppliers or employees;
- (d) reasonable indication that the Material will not be delivered within the time specified in the Purchase Order;
- (e) invoicing which is incorrect; or
- (f) overcharges in violation of the terms and conditions of this Agreement.

Payment does not constitute acceptance of any defective or non-conforming Material or otherwise relieve Supplier of any obligation under the contract.

## **ARTICLE 10 – DELEGATIONS; SUBCONTRACTS; ASSIGNMENT**

A. Supplier shall not, without the prior written authorization of Company, assign this Agreement or any of its rights under this Agreement, nor delegate any of its duties without the prior written consent of Company. Any assignment or attempt to make such assignment shall be null and void. Supplier shall not, without the written consent of the Company, make any agreement with any third party for furnishing any of the completed or substantially completed items covered by this Agreement.

B. Company may assign this Agreement, in whole or in part, (i) to a successor of all or substantially all of Company's relevant assets, or (ii) to an Affiliate; otherwise, neither party shall, without the consent of the other, which consent shall not be unreasonably withheld, conditioned or delayed, assign this Agreement in whole or in part hereunder.

C. If Supplier shall cause any part of the work to be performed by a sub-contractor, the provisions of this Agreement shall apply to such sub-contractor and its officers, agents or employees in all aspects as if they were employees of Supplier, and Supplier shall not thereby be discharged from any of its obligations and liability hereunder, but shall be liable hereunder for all acts and omissions of the sub-contractors. Nothing hereunder shall create any contractual relationship between Company and any subcontractor or any sub-subcontractor.

The Supplier shall submit a list of those work items which it plans to subcontract and the names of Supplier's subcontractor proposed for the work together with all materials for an evaluation by Company's Corporate Security Group. Supplier's subcontractor may not be changed except at the request of or with the written approval of Company, which shall not be unreasonably withheld. The Company shall promptly notify the Supplier in writing if, after due investigation, Company has reasonable objection to any subcontractor on such list and does not accept it.

Supplier shall assign to Customer any subcontractor warranties applicable to the services that extend beyond the applicable warranty period upon the expiration or termination of such warranty period. Supplier shall assign any subcontractor warranties applicable to the services to Customer if Supplier becomes insolvent or files for bankruptcy.

## **ARTICLE 11 – SET-OFF**

Company may set off against any amount payable to the Supplier under this Agreement any claim or charge it may have against Supplier.

## **ARTICLE 12 - INSPECTION**

The Company (and/or its designee) reserves the right to inspect the Material prior to shipment. Such inspection does not relieve the Supplier of its guarantees or responsibility to furnish satisfactory Materials. It is furthermore understood to be Company's privilege to waive inspection at point of manufacture without prejudice to its right to decline acceptance. Except as to items purchased from stock, items supplied hereunder and materials and components incorporated therein shall be subject to inspection at Company's option by Company or its designee during and after manufacture. All Material is subject to inspection and acceptance tests at place of manufacture, or at destination, or at both places,



by the Company's representative. Rejected Material shall not be submitted for acceptance without concurrent notice of their prior rejection.

### **ARTICLE 13 - WARRANTY**

The Supplier warrants the Material shall be new, free of defects in material, design, engineering and workmanship as conditioned herein for a period of seven (7) years from date of receipt or the term stated in *Schedule E*. During said warranty period, the Supplier shall repair or, at its option, replace of the defective Material without any cost to the Company, including, without limitation, costs for de-installation or costs related to shipping.

In the event Supplier is unable to satisfactorily repair the defect through modification, repair or replacement, the Company may return the defective Material, and, at its option, obtain a credit or refund of the purchase price.

The Supplier may advise the Company of any preferred routing for return of rejected Material and whether or not the shipment should be protected by insurance or full declaration of value at the time of acceptance of this order. In the absence of such information from the Supplier regarding such shipment, the Company reserves the right to declare full valuation or insurance (whichever is applicable) for the benefit of and at the expense of the Supplier.

### **ARTICLE 14 – SAFETY**

Supplier warrants that the Material will conform to the applicable occupational safety and health standards promulgated pursuant to the Federal Occupational Safety and Health Act of 1970 and which are in effect on the date that the Supplier enters its acknowledgments of Company's order.

### **ARTICLE 15 – PATENTS AND OTHER INTELLECTUAL PROPERTY; INDEMNIFICATION**

Supplier represents and warrants that the purchase by Company of and the use by Company of any Material, including, without limitation, the Work Product, will not infringe any United States or foreign patent or other intellectual property right, and Supplier shall defend, indemnify and hold Company harmless against all claims, judgments, decrees, costs and expenses resulting from any such alleged infringement. Supplier shall at its own expense defend, or settle any claim, suit or proceedings brought against Company, so far as based on an allegation that any Material, including, without limitation, Work Product, or any part thereof furnished hereunder constitutes a direct or contributory infringement of any claim of any United States or foreign patent, copyright or other intellectual property right. In case the Materials, including, without limitation, Work Product or part thereof furnished hereunder becomes the subject of any claim, suit or proceeding that such Material, including, without limitation, Work Product or part infringes any United States or foreign patent, copyright or other intellectual property right or if the use or sale of such Material, including, without limitation, Work Product or part thereof is enjoined, Supplier shall, at Company's option, and at Supplier's own expense, either: (a) procure for Company the right to continue using said Material, including, without limitation, Work Product, or part thereof; (b) replace it with non-infringing Material, including, without limitation, Work

Product, that is functionally equivalent to the Material, including, without limitation, Work Product, being replaced and satisfactory to the Company, or (c) modify it so it becomes non-infringing, so long as it remains functionally equivalent and satisfactory to the Company.

## **ARTICLE 16 – TERMINATION FOR CAUSE**

Company, reserving to itself the right to receive such other damages and remedies as it may have pursuant to this Agreement or at law or in equity, has the right to terminate this Agreement, by giving written notice of termination to Supplier of the occurrence of any of the following:

- (a) Supplier defaults in the observance or performance of any covenant, agreement or condition contained in this Agreement required to be kept, performed, or observed by Supplier, if within thirty (30) days after the giving of written notice to Supplier of such failure of performance, Supplier has not cured such failure or if such failure of performance cannot be cured in thirty (30) days, if Supplier has not commenced curing such failure of performance promptly and within such thirty (30) day period is not effectuating such cure with haste and does not cure such failure of performance within a reasonable time, not to exceed, ninety (90) days from receipt of the notice specified herein.
- (b) In the event that Supplier is declared to be bankrupt or insolvent, Supplier makes an assignment for the benefit of creditors, Supplier shall file a voluntary petition in bankruptcy or insolvency or an involuntary petition is filed against Supplier, or a receiver shall be appointed for Supplier and such appointment or bankruptcy or insolvency proceedings, petition, declaration or assignment is not set aside within thirty (30) days.
- (c) There has been a material adverse change in the financial condition of Supplier that affects the ability of Supplier to perform.
- (d) Supplier assigns or attempts to assign its rights or obligations under this Agreement or any part thereof to any third party without the prior written consent of the Company.
- (e) Supplier (i) fails or refuses to comply with any Applicable Laws or Applicable Permits, and (ii) either (A) within five days after obtaining knowledge of such non-compliance does not commence steps to comply or is not in compliance with such Applicable Laws or Applicable Permits within a reasonable period of time thereafter, or (C) Company faces any civil or criminal action or penalty as a result of such non-compliance by Supplier.
- (f) Any Data Security Breach as defined in the Data Security Rider, as applicable.

Termination of a scope of work or a Purchase Order under this Article 16 does not terminate this Agreement unless expressly stated in the termination notice from Customer and/or Company.

Supplier, reserving to itself the right to receive such other damages and remedies as it may have pursuant to this Agreement or at law or in equity, has the right to terminate this Agreement, by giving written notice of termination to Company that Company defaults in the observance or performance of any covenant, agreement or condition contained in this Agreement required to be kept, performed, or observed by Company, if within thirty (30) days after the giving of written notice to Company of such

failure of performance, Company has not cured such failure or if such failure of performance cannot be cured in thirty (30) days, if Company has not commenced curing such failure of performance promptly and within such thirty (30) day period is not effectuating such cure with haste and does not cure such failure of performance within a reasonable time, not to exceed, ninety (90) days from receipt of the notice specified herein; provided, for purposes of clarity, in no event shall Contractor be entitled to terminate this Agreement for a payment default until at least ninety-90 days' prior notice to the Company and opportunity to cure.

#### **ARTICLE 17 – TERMINATION FOR CONVENIENCE**

Company may suspend or terminate this Agreement in whole or in part by giving the Supplier fourteen (14) business days' prior written notice. In such event the Company shall make payment to the Supplier for all Material delivered prior to such termination reasonably allocable to this Agreement, under recognized accounting practice, less disposal or retention value of termination inventory. Supplier shall make commercial reasonable efforts to mitigate the amount to be paid by Company pursuant to this provision. This provision shall not be deemed to limit or otherwise affect the Company's right to terminate this Agreement for breach or default by the Supplier.

#### **ARTICLE 18 – INSURANCE AND GENERAL INDEMNIFICATION**

- (a) Insurance. Supplier shall maintain insurance in accordance with the requirements as set forth in *Schedule G* and the cyber insurance requirements set forth in *Schedule H*. An insurance certificate must be mailed to Customer prior to starting services.
- (b) General Indemnification. The Supplier shall defend, indemnify, and hold harmless, to the fullest extent permissible by law, the Company, its Affiliates, agents, employees, shareholders, managers, members, partners, officers, directors successors, permitted assigns, and all affiliated and subsidiary companies, corporations, trusts, partnerships, joint ventures (including joint venture partners), associated companies, associations, subsidiaries of the foregoing and individuals which are now or may hereafter be owned, controlled, operated, or directed by or a subsidiary to Company, from and against any and all claims, demands, damages, losses, and expenses, including reasonable attorney's fees, arising out of or resulting from the performance of this Agreement, provided that any such claim, damage, loss, or expense (a) is attributable to bodily injury, sickness, disease, or death, or to injury to or destruction of tangible property, or (b) is caused in whole or in part by a negligent act or omission of the Supplier or any of its officers, agents, representatives, subcontractors, anyone directly or indirectly employed by any of them, or anyone for whose acts any of them may be liable. In furtherance of the foregoing indemnification and not by way of limitation thereof, the Supplier hereby waives any defenses or immunity it might otherwise have under applicable worker's compensation laws or any other statute or judicial decision (including, for Work or services to be conducted in Maine, without limitation, *Diamond International Corp. v Sullivan & Merritt, Inc.* 493 A2d. 1043 (Me 1985)) disallowing or limiting such indemnification, and the Supplier consents to a cause of action for indemnity.

## ARTICLE 19 – FORCE MAJEURE

For purposes of this Agreement, “Force Majeure Event” means, with respect to a Party, any event or circumstance, regardless of whether it was foreseeable, that was not caused by that Party or the negligence of that Party and that prevents a Party from complying with any of its obligations under this Agreement, and that the Party claiming the occurrence of such event has furnished the other Party with prompt notice when it appears that such cause will result in non-performance or shall threaten to impair such Party’s performance, except that a Force Majeure Event will not include a strike, workforce unavailability, or other labor unrest that affect only one Party, late delivery or breakage of equipment or materials (except to the extent due to a Force Majeure event otherwise excusable hereunder), lack of funds or change in economic circumstance, a failure of performance of any third party (except to the extent due to a Force Majeure event otherwise excusable hereunder), failure to properly apply for any permits for which Supplier is responsible in a timely manner or to perform any conditions therein, an increase in prices, a change in market demand, a change in law, weather or climatic conditions within the range of severity as recorded by the *National Oceanic and Atmospheric Administration* over the past twenty-five (25) years in the vicinity of the Site or elsewhere, or actions of a Governmental Authority with respect to the Supplier’s compliance, or failure to comply, with Applicable Laws, Permits, or Governmental Authority-imposed measures. Force Majeure may include the following events, (a) war, hostilities (whether war be declared or not), invasion, act of foreign enemies in each case within the country; (b) rebellion, terrorism, revolution, insurrection, military or usurped power, or civil war in each case within the country; (c) riot, commotion, disorder, strike or lockout in each case within the country, by persons other than the Supplier, the Supplier's Personnel, Subcontractors and other employees of the Supplier; (d) ionising radiation or contamination by radio-activity, except as may be attributable to the Supplier's use of such radiation or radio-activity; or, (e) natural catastrophes, such as earthquake, volcanic activity, hurricane or typhoon (but not any other weather, climate or metocean conditions). Supplier shall have used its commercially reasonable efforts to remedy the delaying cause or condition and recommence performance, and has furnished the Customer with prompt written notice when it appears that such cause will result in non-performance or shall threaten to impair Customer’s ability to operate. Customer shall have the right, at its option and without being under any liability to Supplier, to cancel, by notice in writing to Supplier the portion or portions of the Agreement so affected and to take such compensatory action as may be necessary. Correspondingly, Customer shall be excused for failure of performance herein due to any cause beyond its control and without its fault or negligence. Upon occurrence of a Force Majeure Event, the nonperforming Party shall promptly notify the other Party of occurrence of that Force Majeure Event, its effect on performance, and how long that Party expects it to last. Thereafter the nonperforming Party shall update that information as reasonably necessary. During a Force Majeure Event, the nonperforming Party shall use reasonable efforts to limit damages to the other Party and to resume its performance under this Agreement. If the Force Majeure Event extends for more than twenty (20) days and if the Supplier cannot reasonably reschedule or perform any affected element of this Agreement, the Customer shall be entitled to terminate this Agreement upon notice to the Supplier. Supplier shall furnish timely reports every ten (10) Business Days during the continuation of each Force Majeure Event with respect thereto and whenever such Force Majeure Event has ceased. If a Force Majeure Event materially affects Supplier’s schedule for performance hereunder, Supplier may request an equitable adjustment and the Parties agree to memorialize schedule changes in a change order. If the effects of a Force Majeure Event last longer than twelve (12) months, that shall entitle Customer to terminate the Agreement or Purchase Order, as the case may be.

*AVANGRID Service Company and Supplier expressly agree, notwithstanding any provision in this Agreement to the contrary, that: (i) a COVID-19 pandemic exists worldwide as of the execution date of this Agreement; (ii) the existence of such pandemic, and its effects, now, and for the duration of Supplier's performance under the Agreement, including, without limitation, effects upon pricing, schedule, quantities or specifications, if any, shall not be cause for Supplier to rely upon, invoke, or avail itself to, any rights or remedies under this Agreement, at law, or in equity, for a claim, or an adjustment to the price, schedule, quantities, specifications, or other material terms of this Agreement, including the rights and remedies set forth in the Force Majeure provision of this Agreement; (iii) the material terms of this Agreement, particularly terms relating to price, schedule, quantities, availability and specifications, take into consideration, and fully account for, the existence of such pandemic and its effects, now, and for the duration of Unlimited Technology, Inc 's performance under the Agreement; and (iv) such pandemic shall not render Supplier unable to fulfill any of its obligations under the Agreement. Supplier shall not have any claim, action or cause of action against AVANGRID Service Company in connection with such pandemic, including any claim for frustration of purpose, change in circumstances, economic balance or impossibility. This provision shall survive the completion or earlier termination of this Agreement.*

#### **ARTICLE 20 - SUBSTITUTION**

No substitution will be permitted under this Agreement except on specific written authority of the Company, granted in Company's sole and absolute discretion.

#### **ARTICLE 21 – INDEPENDENT CONTRACTOR**

Supplier shall at all times be an independent contractor and responsible for all acts or omissions of its agents, employees, and subcontractors. Supplier shall at all times control and retain the right to control its performance, no act or order of Company shall be deemed to be the exercise of supervision or control of performance hereunder.

#### **ARTICLE 22 – AUDIT RIGHTS**

Upon fourteen (14) days advanced written notice, the Company may audit, or cause to have audited, any and all items related to any aspect of this Agreement in order to assure Supplier's compliance. These items shall include, but not be limited to, property, books, records, and computerized data files. This provision shall remain in effect for two (2) years following final payment for the Material covered under this Agreement. Company also reserves the right to perform an onsite audit at Supplier's facility, used in providing the Service to Company, to evaluate processes and procedures critical to the distribution of Material for Company. All results of these audits must be kept confidential between the Parties and their agents.

#### **ARTICLE 23 - LIENS**

The Supplier represents and warrants that it has good and exclusive title to all Material delivered pursuant to this Agreement and that the Material to be supplied hereunder is free and clear of all liens, encumbrances and claims. The Company may withhold payment pending receipt of evidence in form and substance satisfactory to it of the absence of such liens, claims and encumbrances. Supplier shall,

at its own expense and cost, defend (at Company's option), indemnify, and hold harmless Company from and against all liens, encumbrances, or claims.

Supplier shall take all action reasonably necessary to discharge, remove, or satisfy any lien filed against any property of the Company or its affiliate(s), or any portion thereof, arising from any work, labor, services, or materials claimed to have been performed or furnished for, or on behalf of, the Supplier or any person or entity by or through the Supplier. Supplier shall forthwith take such action necessary to discharge, remove, or satisfy any such lien filed against the property of the Company, including but not limited to posting of a bond. If the Supplier shall fail to discharge, remove, or satisfy any such lien within ten (10) days after notice of the existence of such lien has been provided by the Company, the Company shall have the right, but not the obligation, to pay the amount of such lien, or discharge the same by deposit or bonding, and the amount so paid or deposited, or the premium paid for such bond, with interest at the maximum allowable by law, may be set-off against any payment due Supplier under this Agreement.

#### **ARTICLE 24 - TAXES**

The Supplier shall timely and properly remit to the applicable Government Authority all Sales Taxes (as defined below) collected by the Supplier from the Customer. Customer shall be responsible for and pay any sales tax, use tax, excise tax, gross receipts tax, or any other transaction tax (collectively, "Sales Taxes") that are due and payable under applicable Laws with respect to any payment by it of Contract price to the Supplier to the extent the amount of such Taxes has been included, as a separate line item or items, on an appropriate invoice from the Supplier relating to the applicable payment of the Contract price and Customer shall reimburse the Supplier for "Sales Taxes" paid by the Supplier in connection with its performance of the services under the Contract; provided, however, the Customer shall not be responsible, or reimburse the Supplier, for any such Taxes to the extent an exemption from (including a reduction of) such Taxes is available under applicable laws. Each Party will be responsible for its own income, employment, and property taxes.

## **ARTICLE 25 – SPARE PARTS**

Supplier agrees to provide spare parts at the fair market price, with no minimum billing, for 10 years, or for the design life of the Material purchased, whichever is greater or any other term specified in *Schedule E*.

## **ARTICLE 26 - SEVERABILITY**

In the event any provision hereof shall be declared invalid, that provision shall be deemed severable from the remaining provisions of this Agreement, which shall remain in full force and effect.

## **ARTICLE 27 – COMPLETE AGREEMENT**

This Agreement, together with all attachments, schedules, and appendices, shall constitute the complete agreement between the parties with respect to the subject matter of this Agreement. All prior communications with respect to this Agreement, whether oral or written, are superseded by this Agreement. This Agreement may be executed in duplicate, each of which shall be deemed to be an original, but which together shall constitute one and the same instrument.

## **ARTICLE 28 - CONFIDENTIALITY**

Each Party (a “Receiving Party”), and its employees and agents, shall treat any information, (including any technical information, experience or data) regarding the other Party’s (a “Disclosing Party”) plans, programs, plants, processes, costs, equipment, operations, which may be disclosed to, or come within the knowledge of, Receiving Party its employees and agents in the performance of this Agreement, as confidential, and will not use or disclose this information to others, during the term of this Agreement, and for three (3) years thereafter, except as is necessary to perform its obligations hereunder, without Disclosing Party’s prior written consent. The provisions of this Article shall not apply to any information referred to in this Section which (i) has been published and has become part of the public knowledge through no effort by Supplier, its employees, or agents, (ii) has been furnished or made known to Receiving Party or Receiving Party’s Affiliates by third parties (other than those acting directly or indirectly for or on behalf of the Disclosing Party) as a matter of legal right and without restriction on disclosure, (iii) was in Receiving Party's possession prior to disclosure by the Disclosing Party and was not acquired by Receiving Party or Receiving Party’s Affiliates, its employees and agents directly or indirectly from the Disclosing Party or, (iv) is required by law or by any other governmental regulatory authority to be disclosed.

Any information, which is supplied by the Receiving Party to Disclosing Party under this Agreement, will be similarly restricted. Disclosing Party will not disclose such information to others or publish it in any form at any time; provided, however, that notwithstanding the foregoing, Disclosing Party may disclose any such information to its Affiliates, to its employees, and consultants, to any regulatory agencies or instrumentalities when such disclosure is necessary, or otherwise required by law.

Each Party agrees that it will cooperate with the other in an effort to minimize the amount of such information, which is required by law or governmental regulatory authority to be disclosed in any such case, and to make reasonable efforts to secure confidential treatment of such information.

In no event shall either Party's name and/or logo or the name and/or logo of its Affiliates be used, whether written or verbal, duplicated, reproduced by any means whatsoever without the prior written permission of the other Party.

#### **ARTICLE 29 - TITLE**

Complete legal and equitable title of each item of hardware and other physical Material covered by this Agreement shall pass to Company immediately upon delivery at warehouse and/or job site. This provision shall apply irrespective of any terms of payment specified in this Agreement. Passage of title pursuant to this provision shall not release or waive any continuing or subsequent responsibility of Supplier under this Agreement.

#### **ARTICLE 30 - PUBLICITY**

Supplier shall not issue, nor permit to be issued any press release, advertisement or literature of any kind or conduct or permit to be conducted any interview or news conference, referring to this Agreement or the Materials hereunder, except upon prior written consent of the Company.

#### **ARTICLE 31 – GOVERNING LAW**

All questions concerning the interpretation, validity and enforceability of this Agreement and of its terms and conditions, as well as questions concerning the sufficiency or other aspects of performance under the terms or conditions of this Agreement, shall be governed by the law of the State of New York, without reference to its conflict of law provision and any action or proceeding brought in connection therewith, will be brought in the appropriate court located in the State of New York. The Parties hereby irrevocably consent to the jurisdiction of such court and hereby waive, to the fullest extent permitted by, any objection which they may now or hereafter have to the venue of any such dispute related to or arising out of this Agreement brought in such court or any defense of inconvenient forum for the maintenance of such dispute. Each Party agrees that a judgment in any such dispute may be enforced in other jurisdictions by suit on the judgment or in any other manner provided by law.

#### **ARTICLE 32 – EMPLOYEE SOLICITATION**

Each Party understands and acknowledges that the other Party has expended and continues to expend significant time and expense in recruiting and training its employees and that the loss of employees would cause significant and irreparable harm to such Party. To the maximum extent permitted under applicable laws, the Parties agree and covenant not to directly or indirectly solicit, hire, or recruit, or attempt to solicit, hire, or recruit—any employee who has been employed by the other Party or its Affiliates during the term of this Agreement, with whom such Parties has had contact in connection with the negotiation, execution, or performance of this Agreement (collectively, "Covered Employee"), or induce the termination of employment of any Covered Employee for a period of one (1) year, beginning on the employee's last day of employment with a Party or one (1) year after the term of this Agreement, whichever is sooner in the applicable case, except with the prior written consent of the Customer, and Supplier shall not induce or attempt to induce, directly or through an agent or third party, any such Covered Employee to leave the employ of the Customer or its Affiliates. As used herein, the term "Affiliate" shall mean any person or entity controlling, controlled by, or under common control with a Party through majority stock or other ownership interest, direct or indirect. Notwithstanding the



foregoing, nothing in this clause shall either (i) limit a Party from employing any person who contacts such Party on his or her own initiative and without any solicitation by such Party specifically directed to such employee, or (ii) directly or indirectly prohibit or restrict either Party from soliciting or hiring another Party's current or future employees to the extent such prohibition or restriction is prohibited or impermissible under applicable laws.

### **ARTICLE 33 – ETHICS**

Supplier shall comply with the AVANGRID Suppliers' Code of Ethics ("Suppliers' Code of Ethics") in connection with its performance under this Agreement. The Suppliers' Code of Ethics can be found at the AVANGRID website ([www.avangrid.com](http://www.avangrid.com)).

### **ARTICLE 34 – NO DISPUTE**

Supplier covenants that it is not aware of any pending billing dispute or other contractual dispute (pursuant to current contracts or contracts no longer in effect) or any pending or threatened litigation between Supplier and/or any of the Supplier's Affiliates and Customer and/or any of Company's Affiliates.

### **ARTICLE 35 – SECURITY REQUIREMENTS**

Supplier shall comply with Company's Security Requirements in their performance of work under this Agreement. Supplier hereby agrees to comply with the terms and conditions of the Company's (i) Background Check Requirements attached hereto as Schedule I and made an integral part hereof, and (ii) Data Security Rider attached hereto as Schedule H and made an integral part hereof in its performance of its obligations under this agreement, including, without limitation, in connection with the Materials.

#### **Company Information:**

(1) The term "Company Information" means all information, in any form: (i) furnished or made available directly or indirectly to Supplier by Company or its Affiliates, or otherwise obtained by Supplier from Company or its Affiliates, or (ii) obtained from Company or Company's Affiliates in connection with the performance of its obligations under this agreement, including, without limitation, in connection with the Materials.

(2) Company Information shall be and remain the property of Company or its Affiliate(s), as appropriate. Supplier shall not possess or assert any lien or other right against or to Company Information. No Company Information, or any part thereof, shall be sold, assigned, leased, or otherwise disposed of or to third parties by the Company or commercially exploited by or on behalf of Supplier, its employees, or agents.

(3) Upon Company's request, the termination or expiration of this Agreement for any reason (including termination for cause) or, with respect to any particular Company Information, on such earlier date that the same shall be no longer required by Contractor in order to render the services, Contractor shall promptly return to Company such Company Information (including copies thereof) in

a form reasonably requested by Company or, if Company so elects, shall destroy such Company Information.

(4) Supplier shall not use Company Information for any purpose other than to render the services.

(5) Supplier shall establish and maintain safeguards against the destruction, loss, alteration, or unauthorized use of Company Information which are equivalent to those “best practices” employed within the Supplier’s industry.

(6) Supplier shall be familiar with and comply with the requirements of the NERC CIP- 004 for projects at Company and/or its Affiliates’ bulk electric substations (>230Kv).

Supplier shall be familiar with and comply with the requirements of the NERC CIP- 004 for projects or services at or relating to critical cyber assets and critical company operating facilities (“Critical Infrastructure”). The specific CIP Standard follows:

CIP-004 Excerpt:

R3. Personnel Risk Assessment --The Supplier shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency. The personnel risk assessment program shall at a minimum include:

R3.1. The Supplier shall ensure that each assessment conducted includes, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven- year criminal check. The Supplier may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Supplier shall ensure that each assessment conducted includes, at least current residence regardless of duration; and other locations where during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven-year criminal history records check, conduct as much of the seven-year criminal history records check as possible and document the reason the full seven-year criminal history records check could not be performed. The Supplier shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

R3.3. The Supplier shall document the criteria or process to evaluate the criminal history records for authorizing access.

R3.4. The Supplier shall document the criteria, process and the results for verifying that personal risk assessments performed for contracts or service vendors are conducted in accordance in R3.1 through 3.3. The results of personnel risk assessments of its personnel, contracts or service vendors having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.

R3.5. The Supplier shall document criteria, process and the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004 R3.1 to R3.4 within the last seven years.

### **ARTICLE 36 – CONTINUOUS IMPROVEMENT**

Supplier likewise will use its commercially reasonable efforts to improve continuously its performance in all areas. In particular, Supplier will evaluate opportunities for cost/price reductions on items and services ordered and to be ordered and communicate them promptly to the Company. Supplier is expected to advance its economies of production, service, service delivery, material handling and technical prowess at least as fast as other competitors in its industry, and to offer the price and performance benefits of those improvements to Customer, as soon as they become available.

### **ARTICLE 37 - UTILIZATION OF SMALL BUSINESS CONCERN**

Supplier and subcontractors of all tiers must comply with section 52.219-8 of the Federal Acquisition Regulation. This policy requires that small business concerns, veteran-owned small business concerns, service-disabled veteran-owned small business concerns, HUBZone small business concerns, small disadvantaged business concerns, women-owned small business, Alaskan Native Corporation, and Indian tribe concerns shall have the maximum practicable opportunity to participate in the performance of services.

### **ARTICLE 38 - SMALL BUSINESS SUBCONTRACTING PLAN**

Some or all of the goods and services provided hereunder may be used in a contract with the federal government and, therefore, may be subject to the requirements of FAR section 52.219-9. If applicable, each Supplier (except small business concerns) whose contract is expected to exceed \$650,000 (\$1,500,000 for construction) and has subcontracting possibilities is required to submit an acceptable subcontracting plan to the Customer. The plan shall include spending goals with businesses that are defined by the U.S. Small Business Administration as small, women-owned small, veteran-owned small, service-disabled veteran-owned small, HUBZone, small disadvantaged (SDB), Alaskan Native Corporations, and Indian tribes. If the Supplier fails to submit a plan within the time limit prescribed by the Customer, Customer may terminate this Agreement.

The Supplier assures that the clause entitled “Small Business Subcontracting Plan” will be included in all subcontracts, that offer further subcontracting opportunities, and all subcontractors (except small business concerns) who receive subcontracts in excess of \$650,000 (\$1,500,000 for construction) will be required to adopt a plan similar to this plan.

### **ARTICLE 39 - SURVIVAL**

Sections 3, 4, 7, 13, 15, 18, 22, 23, 25, 28 and 32 and all other terms which contain obligations or duties which by their nature are to be or may be performed beyond any termination hereof, shall survive the termination of this Agreement without regard to the reason for termination.

## **ARTICLE 40- CLAIMS/DISPUTES**

- A. Any claims by Supplier relating to this Agreement, must be submitted to the Company or the Compan(ies) in writing within fourteen (14) calendar days of initial occurrence of the basis for the claim. Failure to provide such notification shall be deemed waiver of such claim.
- B. The notice of claim shall include the particulars and shall specify the cause or other basis of the claim, and shall include substantiation of the amount and/or extension to which the Supplier considers itself to be entitled in connection with the Agreement.
- C. dispute or claims by the Supplier shall not affect the diligent prosecution by Supplier of the Materials.
- D. The Parties agree to hold a meeting promptly to attempt in good faith to negotiate a resolution of the Dispute, such meeting to be attended by representatives of the Parties with decision-making authority regarding the Dispute. If, within twenty-one (21) days after such meeting, the Parties have not succeeded in negotiating a resolution of the Dispute, either Party may refer the Dispute to a court under Article 31 which is to be the sole legally binding forum available to the Parties for resolution of a Dispute hereunder.

## **ARTICLE 41 - LIMITATION OF LIABILITY**

To the fullest extent permitted by law, neither Company nor its affiliate(s) shall not be liable for any special, indirect, punitive, exemplary, incidental or consequential damages resulting in any way from the performance of the services hereunder, including lost profits or other business interruption damages, whether based in contract, warranty, tort, negligence, strict liability, or otherwise, and whether suffered by Supplier or by any of its subcontractors, under or in respect to this Agreement or for any failure or performance related to this Agreement howsoever caused.

EXCEPT TO THE EXTENT OF SUPPLIER'S LIABILITY ARISING OUT OF ITS FRAUD, GROSS NEGLIGENCE WILLFUL MISCONDUCT OR ITS INDEMNIFICATION OBLIGATIONS, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE TOTAL AMOUNT OF DIRECT DAMAGES RECOVERABLE FROM A PARTY UNDER THIS AGREEMENT IS LIMITED TO THREE HUNDRED PERCENT (300%) OF THE TOTAL AMOUNT PAID OR TO BE PAID BY COMPANY(IES) UNDER THIS AGREEMENT.

## **ARTICLE 42 - PUBLIC RELEASE OF INFORMATION**

Dates, photographs, sketches, advertising and other information relating to the work under this Agreement, which Supplier desires to release or publish, shall be submitted to the Company for approval two (2) weeks prior to the desired release date. As a part of the approval request, Supplier shall identify the specific media to be used as well as other pertinent details of the proposed release. All releases must have the prior written approval of the Company which approval may be withheld without reason or explanation to Supplier.

## **ARTICLE 43 - SURETY BOND**

The Company shall have the right, at all times, to require the Supplier to furnish a bond covering faithful performance of this Agreement and the payment of all obligations arising hereunder (i.e., Performance Bonds, Mechanics Liens). The Company shall be entitled to approve the amount, form, premium cost, and surety Company issuing such surety bond.

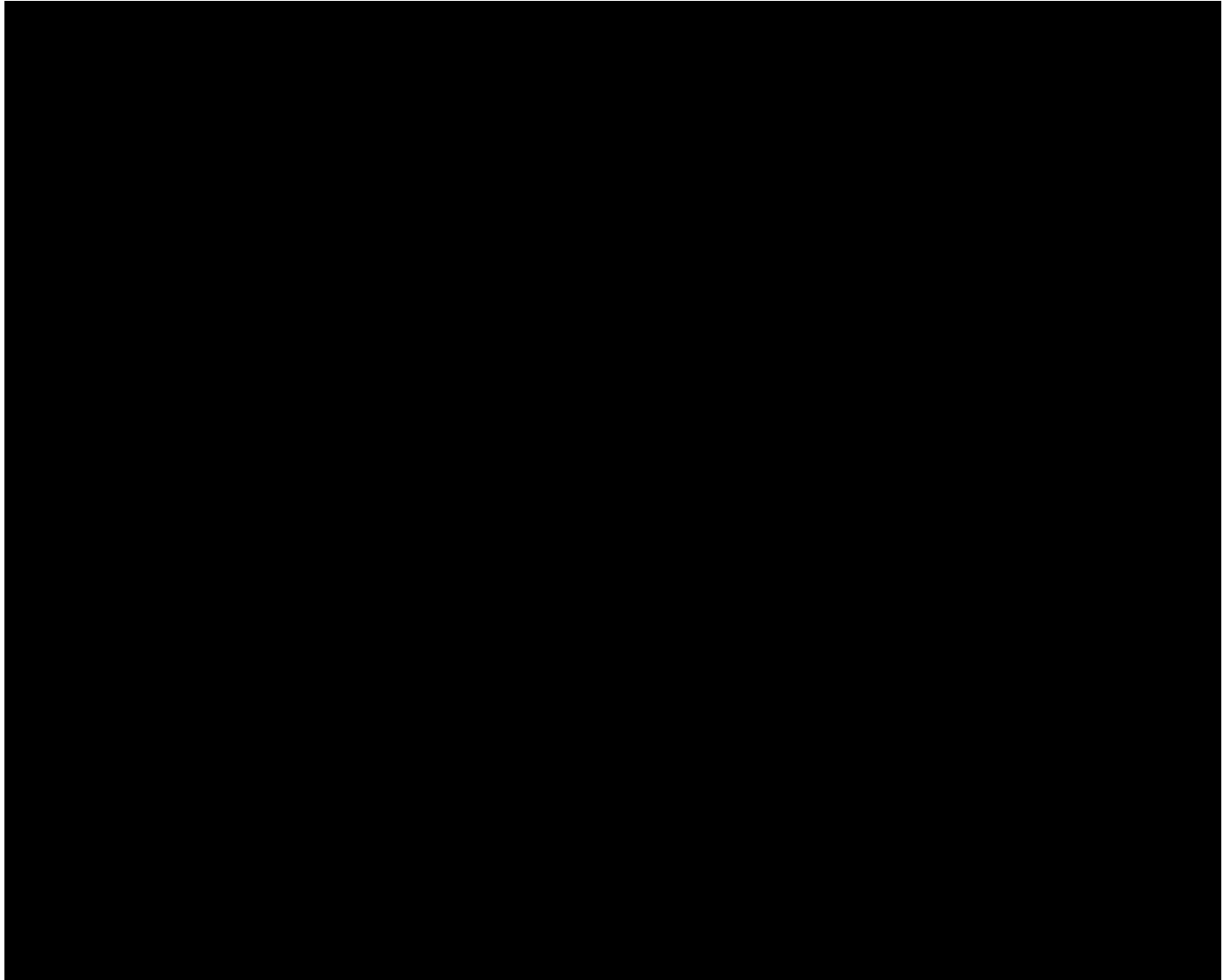
**ARTICLE 44 - GRATUITIES PROHIBITED**

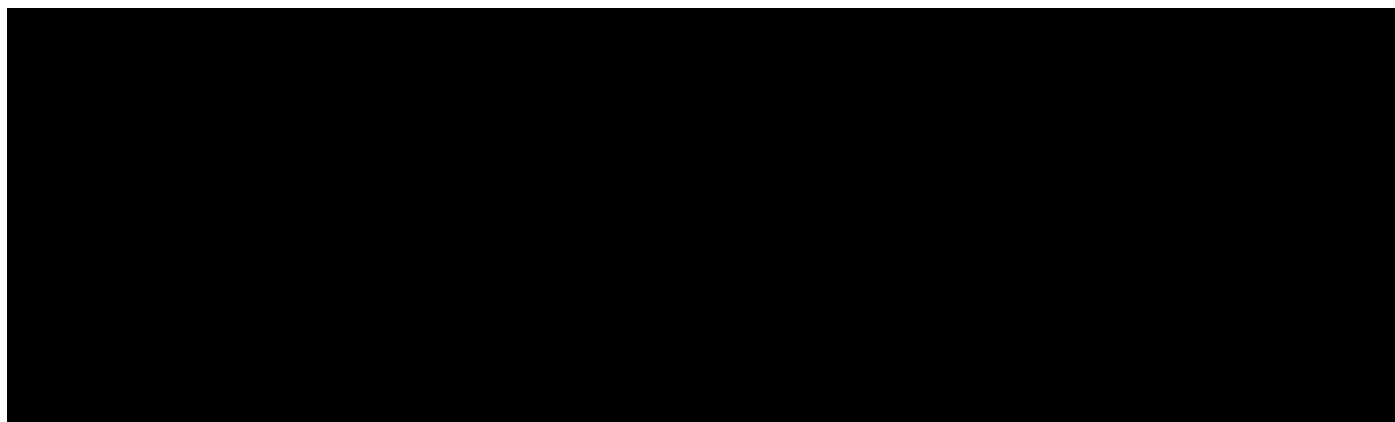
The Supplier shall not, under any circumstances, offer or extend any gratuity or special favor to any employee or agent of the Company or its affiliates or do anything which might reasonably be interpreted as an attempt to influence any employee or agent of the Company in the conduct of their duties.

**SCHEDULE D**

**Pricing Terms**

1. Prices shall remain firm for orders placed during the term of this Agreement. Any requests for price adjustments shall be submitted in writing at least thirty (30) days in advance. Supplier performance will be considered when reviewing any price adjustments, and Customer reserves the right to accept, reject or negotiate any requested price increases.
2. Prices quoted are F.O.B. Destination, freight allowed.
3. Payment Terms are Net sixty (60) days from date of invoice.
4. Spare parts are sold at the same negotiated cost as new parts and services.

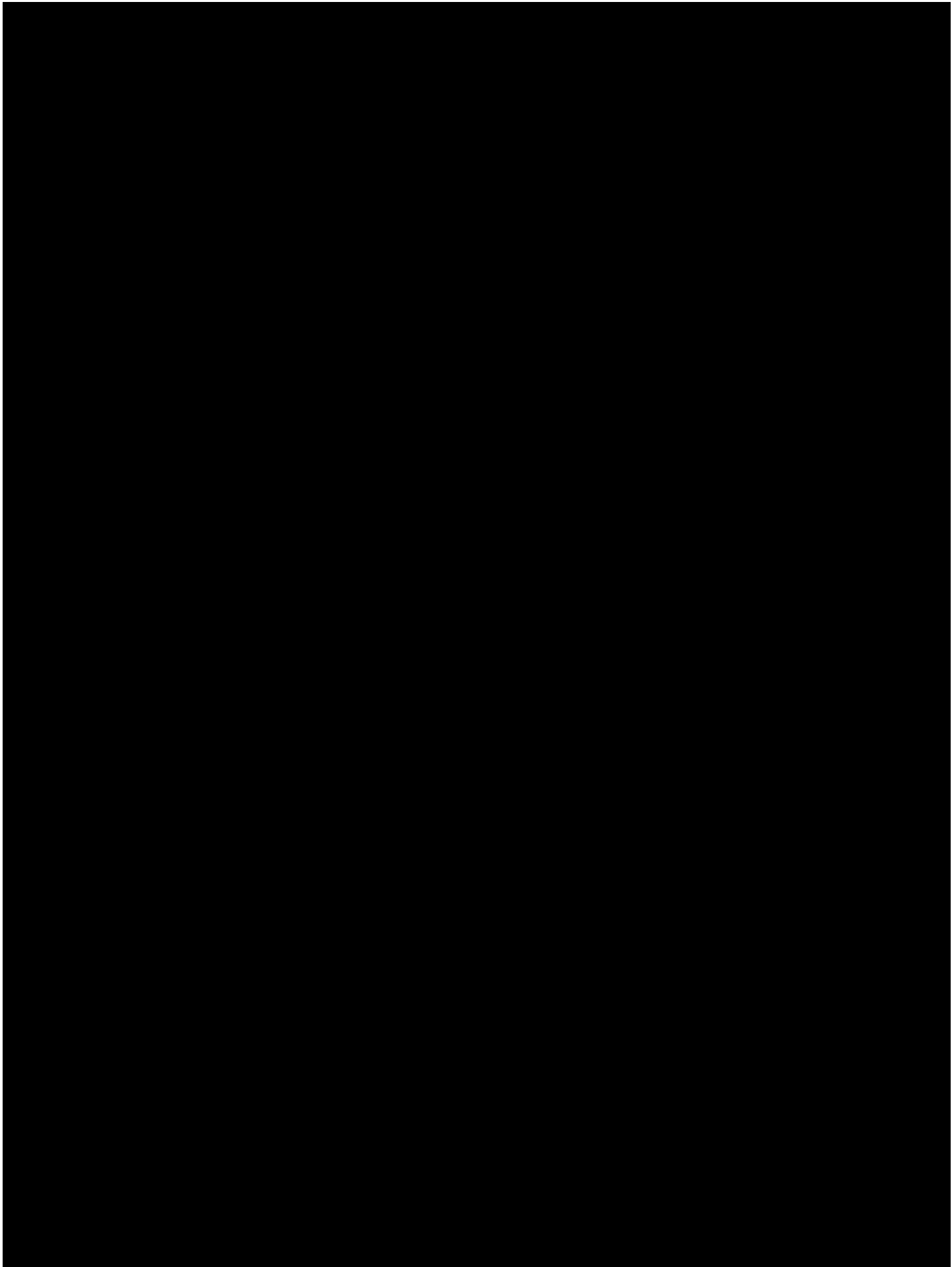


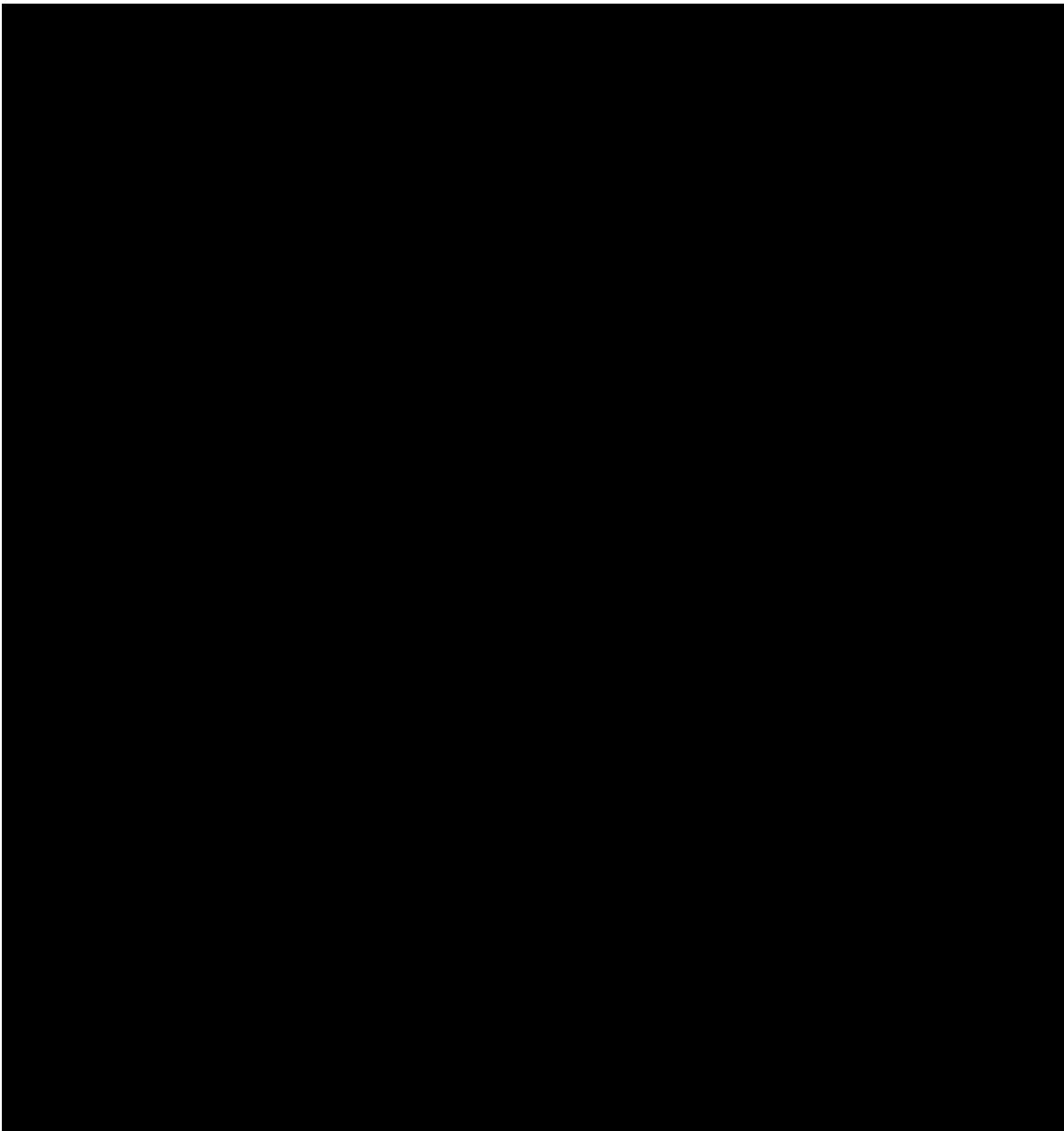


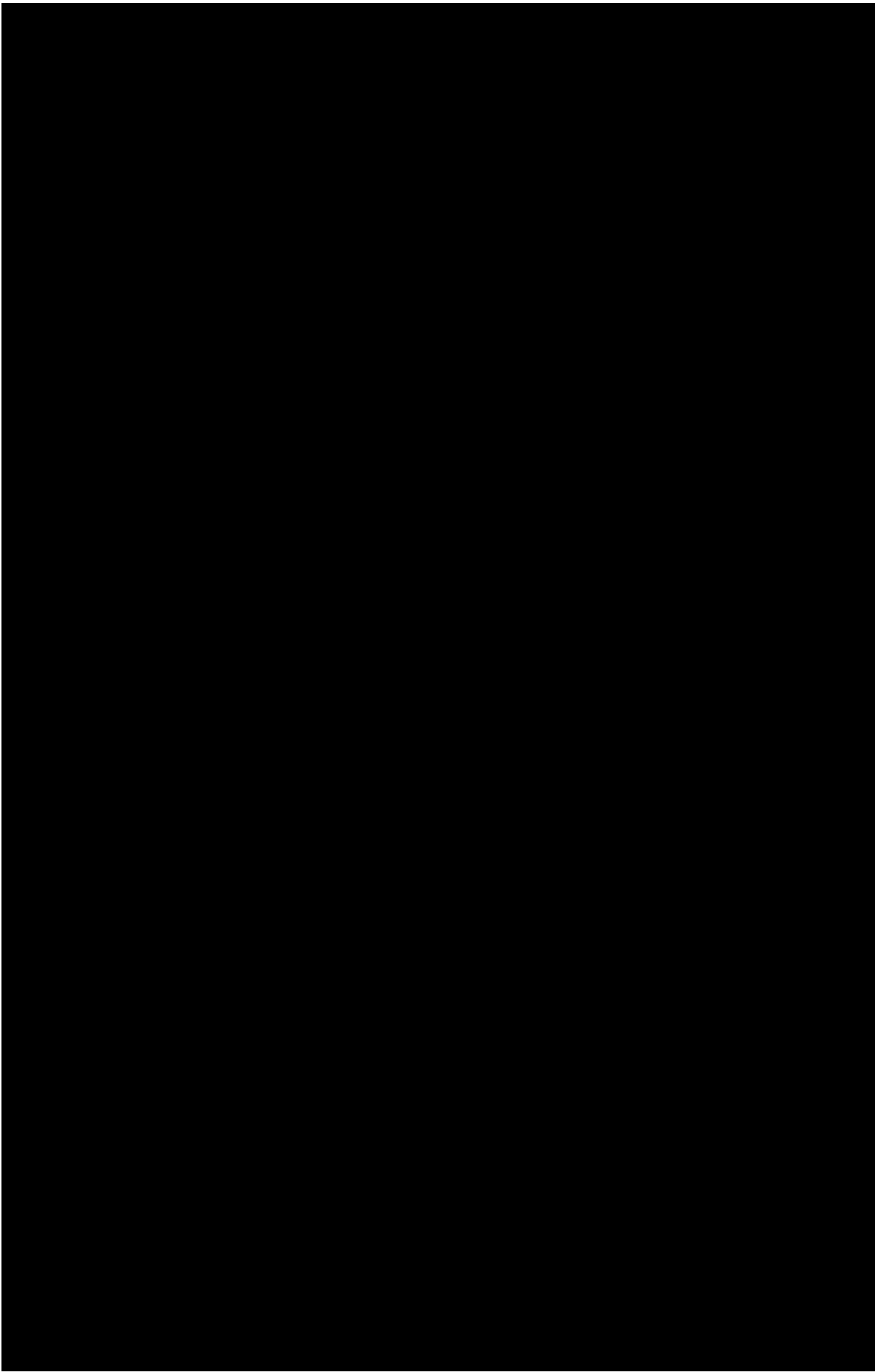


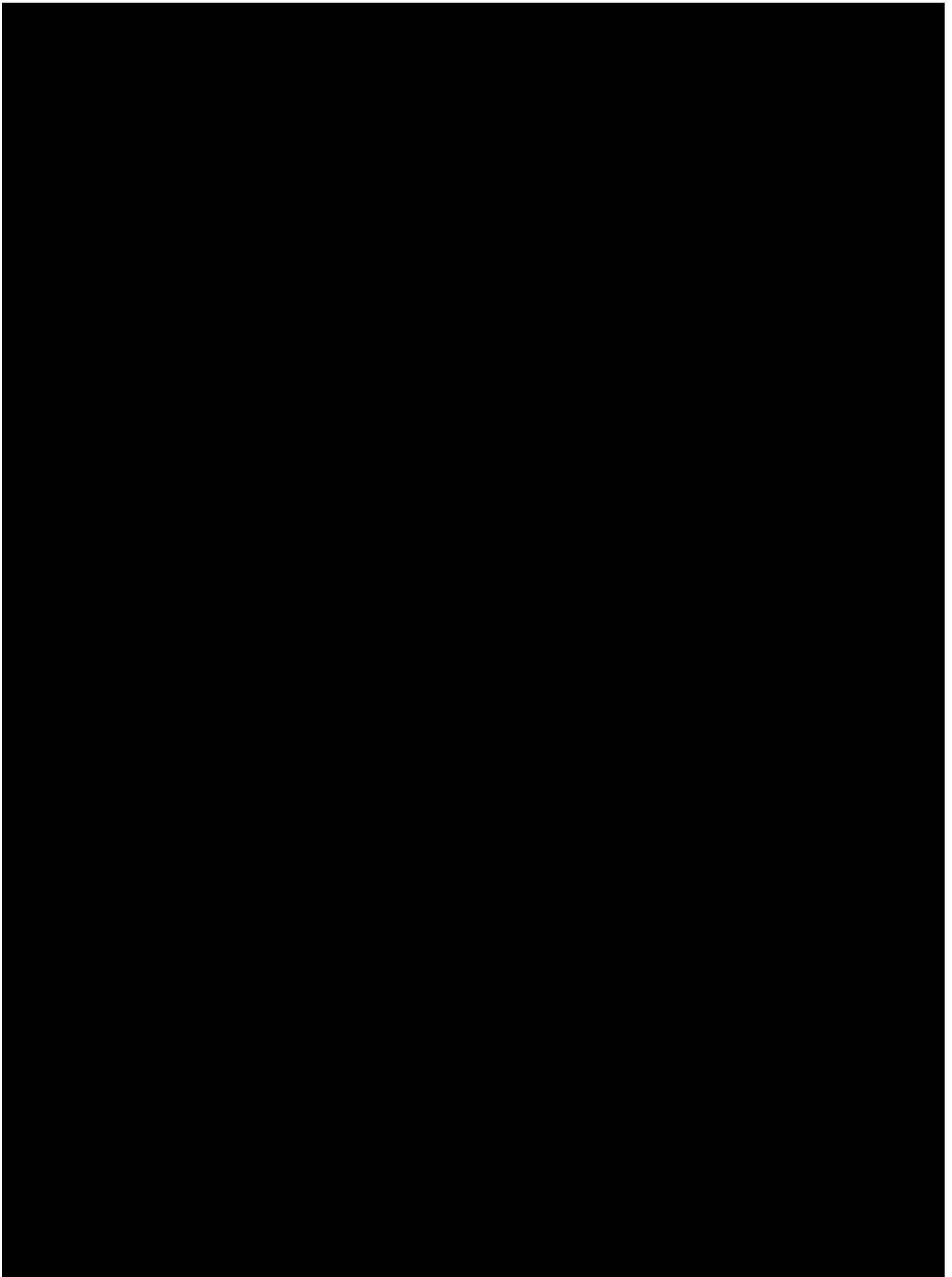


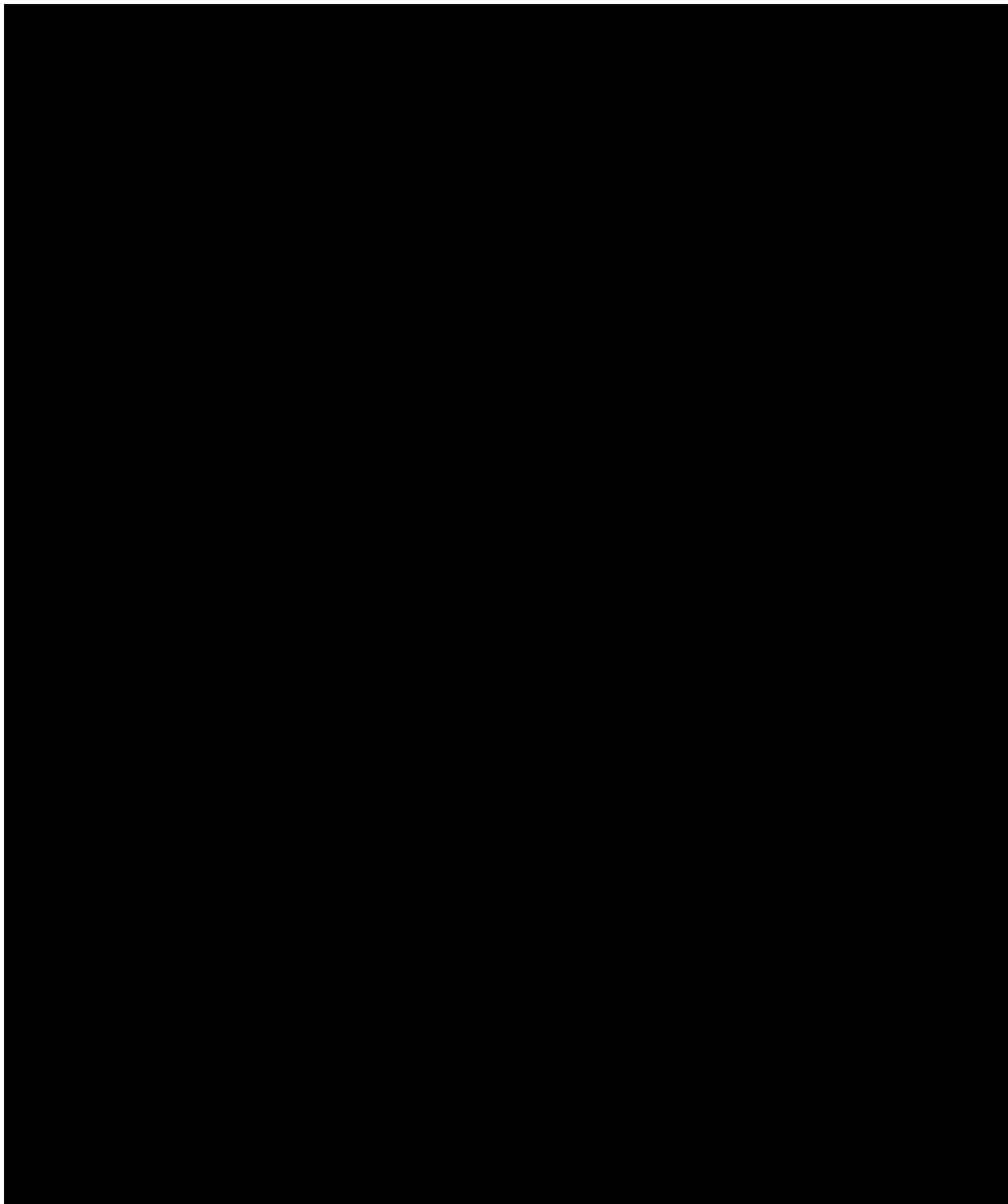












## **SCHEDULE E**

### **Special Conditions**

#### **Key Personnel**

#### **Performance Measurements**

Periodically, Customer may require Review Meetings to discuss supplier performance. Topics of discussion may include, but are not limited to; lead-time, order accuracy, pricing, quality and customer service. Unsatisfactory performance may result in the development of a Supplier performance improvement plan.

#### **Delivery**

Supplier will instruct the transportation company to contact the delivery locations 48 hours in advance to arrange for delivery.

#### **Training**

Refer to Schedule D

**SCHEDULE F**

**Notices**

Along with all other correspondence requirements included in this Agreement, any notice, request, approval or other document required or permitted to be given under this Agreement shall be in writing and shall be deemed to have been sufficiently given when delivered in person or deposited in the U.S. Mail, postage prepaid, addressed as specified herein or to such other address or addresses as may be specified from time to time in a written notice given by such Party, or when email notice has been given with an acknowledgement given by the appropriate Party representative. The Parties shall acknowledge in writing the receipt of any such notice delivered in person.

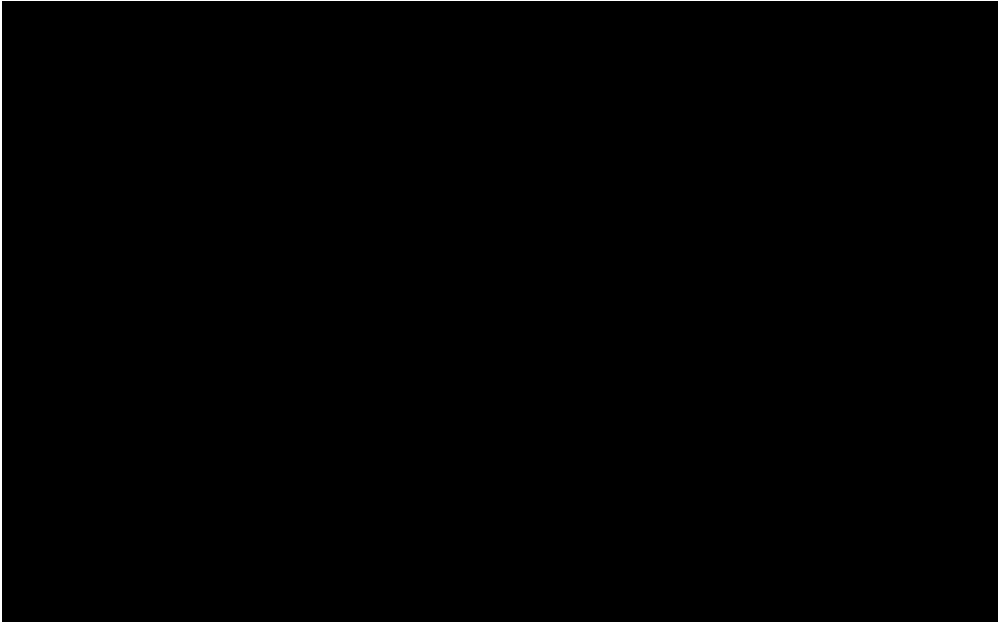
All communications to Customer shall be directed to:

Avangrid Service Company  
Contract Administration  
89 East Avenue  
Rochester, NY 14649  
Phone: 585-724-8028  
Fax: 585-771-2820

With Copy To :  
[Business contact]

1300 Scottsville Rd  
Rochester, NY 14624  
Attention: Josu Menoyo  
Email: josu.menoyo@avangrid.com

All communications to Supplier shall be directed to:





## **SCHEDULE G**

### **Insurance Requirements**

Before commencing services, the Supplier shall procure and maintain at its own expense for a period of two years beyond completion of the services, the insurance types, limits, terms, and conditions listed in Section 1 below. The amounts as specified are in no way limit the indemnification obligations of the Supplier. In addition, for any services that are authorized to be subcontracted, the Supplier shall require each subcontractor to procure and maintain all insurance as outlined in section one.

**IF YOU DO NOT HAVE A CURRENT CERTIFICATE ON FILE WITH CUSTOMER** prior to commencement of services, Certificates of Insurance evidencing Supplier's and/or subcontractor's possession of insurance as outlined in Section 1 shall be filed with Customer and the Companies for its review.

Certificates of Insurance should be mailed to the Procurement Department at the following address:

**AVANGRID Service Company  
Procurement Department/Insurance Cert.  
89 East Avenue  
Rochester, NY 14649-0001**

#### **1. General Insurance Requirements**

Each insurance policy shall be placed with an insurance company authorized to write insurance in the State where the services are to be performed and shall have an A.M. Best Rating of "A- VII" or better.

Each insurance policy shall have defense costs outside of the limits of liability.

Each insurance policy shall include Customer and its Affiliates as additional insureds. Except of any required workers' compensation & employers' liability and professional liability coverages.

Supplier shall provide Customer with 30-day notice of cancellation, except for non-payment of premium and then it shall be 10 days.

Each insurance policy shall be primary and non-contributory with respect to Customer and its Affiliates.

Each insurance policy shall contain a waiver of subrogation in favor of Customer and its Affiliates.

Each insurance policy shall contain a separation of insureds clause.

Each insurance policy shall contain a terrorism provision.

Required Coverages

1) Workers' Compensation and Employers' Liability Insurance:

Coverage A: Statutory

Coverage B:

Bodily Injury by Accident - \$500,000 each Accident

Bodily Injury y Disease - \$500,000 each Employee

Bodily Injury by Disease - \$500,000 Policy Limit

2) Automobile Liability

Combined Single Limit - \$1,000,000 (limits in excess of \$1M can be satisfied by umbrella/excess coverage)

Uninsured/Underinsured – Minimum allowed by State law

Hired/Non-owned liability - \$1,000,000

3) General Liability: ISO Form CG 00 01 or its functional equivalent

Per Occurrence - \$1,000,000

General Aggregate - \$2,000,000

Products Completed - \$2,000,000

Personal and Advertising Injury - \$1,000,000

Endorsements:

Contractual Liability (to the extent covered by insurance Amendment

Explosion, Collapse, Underground Coverage

Independent Contractors Coverage

Broad Form Property Damage

4) Umbrella/Excess Liability: Written on a Substantially Follow Form Basis and Worldwide Coverage

Per Occurrence - \$3,000,000

General Aggregate - \$3,000,000

Products/Completed Operations - \$3,000,000

Personal & Advertising Injury - \$3,000,0000

Underlying Policies: Commercial General Liability, Auto Liability, Employer's Liability

5) Professional Liability:

Per Claim - \$5,000,000

Policy Aggregate - \$5,000,000

Coverage:

Extended Reporting Period – 120 months

Retroactive Date – Date of first design

No Exclusion for environmental impairment liability

## SCHEDULE H

### Data Security Rider

This Privacy and Data Security Rider (the "Rider") is entered into by [REDACTED] ("VENDOR") and Avangrid Service Company. For the purposes of this Rider Avangrid Service Company and any of its affiliates procuring or receiving services, works, equipment or materials under the Agreement shall be hereinafter referred to as the "CUSTOMER".

(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 execution of the Agreement, and establish the obligations and responsibilities of the VENDOR derived from such Processing.

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

(i) "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.

(ii) "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.

(iii) "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.

(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, retention, 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, 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.

(vii) “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.

(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).

(ix) “Agreement” shall mean the Master Materials Agreement between CUSTOMER and VENDOR with respect to which this Rider is being entered into.

(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 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.

(ii) With regards to Company Data, the parties agree that:

- The Processing activities that will be carried out by VENDOR are:
  - o Analyze current telecom network status
  - o Provisioning of new telecom services
  - o Access to stations and service centers
  - o Access to DEV, QA and PROD environments
  - o The categories of Personal Data that will be Processed by VENDOR are:  
Confidential
- The categories of Personal Data subjects whose information will be processed by VENDOR are:
  - o IP Addresses
  - o Protocol configuration parameters
  - o Station and Services Center addresses and POC

- The instructions for the Processing of Personal Data are: All saved data is encrypted, or password protected.
- All sent data is encrypted, or password protected.
- Any encrypted filed password always sent separately

(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, (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:

- (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 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:

- (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;
- (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 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;

(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 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:

- (A) 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;
- (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 Breach or violations; and

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

(vi) 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;

(vii) 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;

(viii) 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;

(ix) 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;

(x) 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 in order 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 in order 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.

(xi) 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;

(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, 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;

(xiii) 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;

(g) At the time of the execution of this Rider, and at any time, upon CUSTOMER's request and a mutual executed Non-Disclosure Agreement, 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 advance notice to VENDOR with the exception of a confirmed breach) of VENDOR's information security protocols related to Company or Personal Data, 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 and a mutually executed Non-Disclosure Agreement, documentation that evidences compliance with the terms of this Rider. CUSTOMER may conduct audits and inspections, either directly or through a third party as agreed under this agreement, and VENDOR agrees to cooperate with CUSTOMER regarding such audits;

(j) 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.

(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 confirmed 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) 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.

(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.

(n) 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 suffered or sustained, 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.

(o) 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.

\*\*\*

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, at all times, 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.

(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 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 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 so as 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 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 of 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 absolutely 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:

(i) Upon a mutually executed Non-Disclosure Agreement, 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) 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.

(k) The Supplier shall immediately notify CUSTOMER of the existence of a confirmed 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:

- (i) Access or attempts to access systems, equipment, applications, files, repositories, devices etc. by unauthorised persons or programs.
- (ii) Disclosing or compromising protected Information including but not limited to credentials, authentication or encryption data.
- (iii) Total or partial loss of data or information for any reason.
- (iv) Uncontrolled distribution: sending information to people who should not receive it.

(v) Loss or removal of computer equipment or storage media, files, repositories or part of their contents.

(vi) Attacks caused by viruses / malicious software that may affect the exchange of information between the VENDOR and CUSTOMER.

(vii) Others: any irregularity or deficiency detected regarding compliance with the safety criteria indicated in this Schedule.

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 claim 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

(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.

## 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 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.

#### 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 in excess of one hour and at all times at the end of the workday.
    - ii. Desktop and laptop computer screens shall be locked by Users at all times 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,**
    - 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.

### **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.
- 1.5.4 Intellectual property, licensing and regulatory requirements shall be observed at all times. 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.

## **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 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 and Blogging 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.
- 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.

- 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.

- 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.

## SCHEDULE I

### Contractor Background Check Requirements

#### Domestic Background Checks

Contractor, at its expense, shall conduct a background check for each employee, agent, representative, contractor, or independent contractor (collectively, "Representatives"), as well as for the Representatives of its subcontractors, who will provide work or services to the Company or who will have access to Company computer systems, either through on-site or remote access (collectively, "Contractor Representatives"). Contractor Representatives, for the purpose of this requirement, include such temporary staff as office support, custodial service, and third party vendors used by Contractor to provide, or assist in the provision of, work or services to the Company hereunder. Contractor's obligations with respect to required background checks shall include those obligations specified for Contractor in the Customer –Contractor Background Check Rule, as such Rule may be revised and/or supplemented from time to time, which Policy is incorporated herein and made part of this Agreement by reference (the "Rule"). Background checks are to be conducted using the Contractor's background check vendor consistent with the process developed with the Company under this Agreement. The minimum Background Check process shall include, but not be limited to, the following checks:

- a. Social Security Number Verification
- b. Motor Vehicle Report
- c. Prohibited Parties Database Search\Debarment Lists
- d. County Criminal History Search in each county where a Contractor or Contractor Representative has resided during the seven (7) years preceding the search.
- e. National Sex Offender Registry.

The Background Check must be completed prior to initial access by Contractor Representative(s) and must, at minimum, meet the criteria specified in this Rule and be repeated every two (2) years for Contractor(s) and Contractor Representative(s) under continuing engagements. Any Contractor Representative who separates employment or other commercial relationship with the Contractor must undergo another Background Check prior to renewed access to the Company. The Company Department charged with managing the relationship with the Contractor hereunder (the "Company Liaison") shall have the right to require more frequent Background Checks of Contractor Representatives or to require checks from other or additional sources than those listed above, and shall have the right to require that the Contractor furnish Background Check results to them. The Company reserves the right to audit Contractor's Background Check process using either a third-party auditor or representatives from the Company's Audit Department or the Company Liaison. All Contractor Representatives are responsible to self-disclose any

misdemeanor or felony conviction(s) that occur during the course of their assignment hereunder within three (3) business days of the conviction. The conviction must be reported to the Contractor and the Company Liaison. If reported first to the Contractor, the Contractor shall notify the Company Liaison and the Company Director of Security within three (3) days of learning of the conviction. If, at any time during the term of this Agreement, it is discovered that any Contractor Representative has a criminal record that includes a felony or misdemeanor conviction, the Contractor is required to inform the Company Liaison who will assess the circumstances surrounding the conviction, time frame, nature, gravity, and relevancy of the conviction to the job duties to determine whether the Contractor Representative will be placed on, or continue in, the assignment with the Company, and consistent with, and to the extent permitted by, applicable state law. The Company may withhold its consent in its sole and absolute discretion. The failure of the Contractor to comply with the terms of this provision shall constitute good cause for termination of this Agreement by the Company, in whole or in part.



### **Foreign Background Checks**

**NERC CIP Access. If applicable (i.e., when IUSA determines that the Contractor engagement is such that compliance with NERC CIP Standards is required), the background check needs to include an identity verification and 7-year criminal history check as more particularly set forth below.**

### Contractor Certification Form

The undersigned agent of [REDACTED] certifies that the employees, contractors, or subcontractors listed below meet the requirements agreed to.

It is the responsibility of the vendor to notify Customer of all personnel changes to include additions as well as voluntary or involuntary terminations. Additions and voluntary terminations are to be communicated within seven (7) calendar days and involuntary terminations must be communicated immediately.

Employee Name	Employer	Date of Last Background Check

Further, I attest that the employees, contractors, or subcontractors listed above working for Customer are in good standing and have been in good standing since their last background check.

[End of Schedule I – Background Check Requirements]