MASTER SERVICES PROCUREMENT AGREEMENT

THIS MASTER SERVICES PROCUREMENT AGREEMENT (the "Agreement") is made this 15th of October 2021 (the "Effective Date") by and between Avangrid Management Company, LLC a Delaware limited liability company, with offices located at One City Center, 5th Floor, Portland, Maine 04101) (hereinafter, "Customer") and [redacted] (hereinafter, "Supplier" or "Vendor" or "Contractor"). Customer and Supplier may be referred to individually as a "Party" and collectively as the "Parties."

WHEREAS, Customer is authorized to assist the utility operating company(ies) identified in ***Schedule A***, attached hereto and made part hereof, in procuring certain services that they may require from time to time in the operations of their respective businesses, including the services described in ***Schedule B***, attached hereto and made part hereof (the "Services"); and

WHEREAS, the Supplier states that it is an established and well-known provider of the Services possessing the skills, qualifications, and experience necessary to perform and manage such Services in an efficient, cost-effective, and controlled manner, with a high degree of quality and responsiveness, and that it has successfully performed similar services for other customers and is willing to provide the Services to the utility operating company Affiliates of Customer 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 the Supplier as a vendor-of-choice for the Services, which shall be procured and awarded in accordance with this Agreement.

NOW THEREFORE, in consideration of the mutual covenants contained herein, and other good and valuable consideration, the 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) "Business Day" – A calendar day other than Saturday, Sunday or a legal, public or bank holiday in the State of Connecticut

(c) "Company" shall mean the company(ies) specified in ***Schedule A***, attached hereto and made part hereof.

(d) "Company Department" shall mean the business unit in AVANGRID that coordinates and manages this Agreement.

(e) "Contract Price" shall mean, in the aggregate, the total maximum dollar amount of all Services pursuant to this Agreement, including, without limitation, any amendment or other modification thereto.

(f) "Day" shall mean a calendar day including Saturday, Sunday or a legal, public or bank holiday in the State of Connecticut.

(g) The "Effective Date" shall mean the date specified in the recitals of this Agreement.

(h) "Industry Standards" - Any of the practices, methods, standards and acts engaged in, or approved by, a significant portion of the independent power industry for the engineering, procurement, construction and maintenance of a static synchronous compensator similar to the Project and located in the United States that, at a particular time, in the exercise of prudent and reasonable judgment by those experienced in the industry, in light of the facts known or that should reasonably have been known at the time a decision was made, could have been expected to accomplish the desired result consistent with good business practices, reliability, economy, health, safety and expedition. "Industry Standards" are not intended to be limited to the optimum practices, methods or acts to the exclusion of all others, but rather to be practices, methods and acts generally accepted in the United States, having due regard for, among other things, manufacturers' warranties, contractual obligations, the requirements or guidance of any Governmental Authority, Applicable Law, applicable NERC reliability requirements and the requirements of applicable insurance policies.

(i) "Intellectual Property " – In relation to any and all technology, software, firmware, know-how, processes, inventions, ideas, discoveries, techniques, algorithms, programs, discoveries, improvements, devices, products, concepts, designs, prototypes, samples, models, technical information, materials, drawings, specifications, mask works, topography and other works of authorship, any and all rights, priorities and privileges relating to intellectual property therein, whether arising under United States, multinational or foreign laws or otherwise, including but not limited to copyright applications and registrations, copyright licenses, patent applications and registrations, patent licenses, trademark applications and registrations, trademark licenses, trade secret rights and all rights to sue at law or in equity for any infringement or other impairment thereof, including the right to receive all proceeds and damages therefrom.

(j) "Project" means the IOC Services project under this Agreement pursuant to which the Supplier will provide the Services.

(k) "Project Completion Date," means the date in which the Project is fully realized to the satisfaction of the Customer and applicable Company(ies).

(l) "Purchase Order" shall mean a purchase order issued by Company or a Company(ies) in accordance with this Agreement.

(m) "RFP" shall mean a request for proposal for all or a portion of the Services by Customer or the Company.

(n) "Scope of Work shall mean the services described in ***Schedule B***, attached hereto and made part hereof.

(o) "Services" shall mean the services and/or related materials described in ***Schedule B***, attached hereto and made part hereof.

(p) "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.

(q) "Supplement" is a written Purchase Order Supplement, signed by the Customer and issued after the execution of this Agreement, authorizing an addition, deletion, or revision in the Services or an adjustment in the Contract Price or the Schedule.

(r) "Term" shall mean the term of this Agreement, as extended or terminated early in accordance with this Agreement.

(s) "Terms and Conditions" shall mean the terms and conditions governing the performance of the Services and related matters pursuant to a Purchase Order, as set forth in ***Schedule C***, attached hereto and made part hereof.

2. PROCESS FOR AWARDING SERVICES

2.1 Customer agrees that, upon a request made to Customer by a Company for assistance in procuring Services, Customer shall, on its own or with the assistance of the Company(ies) requiring the Services, take either of the steps delineated in subsections (a) or (b) toward procuring Services from the Supplier:

(a) Issuance of Purchase Order. Customer or the Company(ies) requesting the Services shall issue to the Supplier duplicate originals of a Purchase Order for the Services incorporating: (i) a scope of work consistent with the standards set forth in ***Schedule B***, (ii) the Terms and Conditions set forth in ***Schedule C***, and (iii) and the pricing terms set forth in ***Schedule D***. Upon receipt of an authorized Purchase Order, Supplier shall commence performance of the Services in accordance with the terms therein.

OR

(b) Issuance of an RFP. (i) Customer or the Company(ies) requesting the Services 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 Services to be provided by the Supplier, consistent with the scope and other requirements specified in the RFP, and (2) Supplier's fees and charges for completing the Services, which will be incorporated as ***Schedule D*** of the Agreement and 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 Services, in their sole and absolute discretion, determine that they wish to award a contract for Services and thereupon select the Supplier's proposal, Customer may elect to issue a Purchase Order and (in such instance) Customer shall forward duplicate original Purchase Orders for the Services (conforming with the requirements of Section 2.1(a), above, 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 performance of the Services in accordance with the terms therein.

2.2 (a) Notwithstanding anything to the contrary in this Agreement or in any Purchase Order or RFP issued hereunder, Customer makes no representation or warranty that Customer or any Company(ies) will issue any Purchase Orders or RFPs, or any minimum dollar volume of Purchase Orders or RFPs, during the Term of this Agreement. Customer or the Company(ies) requesting Services may terminate a Purchase Order or RFP for such Services at any time upon written notice, without penalty or other obligation, prior to commencement of performance of the Services by Supplier in accordance with the terms herein.

(b) Supplier acknowledges and agrees that the issuance of an RFP, Purchase Order, or other document pursuant to this Section 2 by Customer, or any Company(ies), shall not constitute an offer by Customer, or any Company, to purchase Services, and that an enforceable agreement for Services shall result only when Customer or any Company(ies) authorizes a Purchase Order for such Services, processed in accordance with this Article 2, and such Purchase Order is issued to Supplier by Customer, or a Company.

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

(i) The Purchase Order (exclusive of its pre-printed terms and conditions);

(ii) Special Conditions 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 Scope of Services document attached hereto as ***Schedule B***, 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), (vi) and 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. If ***Schedule D*** does not specify a time period, pricing terms shall be fixed for the Term 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 Services awarded to Supplier, Supplier shall include in such calculation the volumes or quantities of Services for all Purchase Orders issued by Customer or any Company(ies) 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 Services executed by the Company(ies) with the Supplier during the preceding calendar year. Customer shall review the reconciliation statement and will notify Supplier of any comments they may have with respect thereto within thirty (30)-days of their receipt thereof. Supplier shall pay to Customer the undisputed portion of any rebates or refunds due the Company(ies) under executed Purchase Orders for Services within five (5) business days following the earlier of: (i) Supplier's receipt of the comments of Customer and Company(ies), 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(ies), that with respect to any Purchase Order for Services issued by any Company(ies) pursuant to this Agreement:

(a) All charges, fees, and expenses, as well as any credits, refunds, or rebates, resulting from Services rendered by Supplier pursuant to such Purchase Order shall be solely for the account of such Company(ies), and neither Customer nor any other Company(ies) 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 Services rendered by Supplier pursuant to such Purchase Order shall be directed to the representative(s) of the Company(ies) identified in such Purchase Order;

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

(d) Pursuant to Article 19 of ***Schedule C***, Supplier shall hold Customer and the other Company(ies) and their respective employees, agents, officers, shareholders, 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 acts of the Supplier and its employees, agents, or representatives pursuant to such Purchase Order.

5. TERM

5.1 This Agreement shall remain in effect until terminated according to Section 5.2(b) below.

5.2 (a) Customer may terminate this Agreement at any time and for any or no reason in accordance with the terms of Article 27 of ***Schedule C*** to this Agreement. Upon the effective date of termination specified in Customer's termination notice: (i) all RFPs, proposals, and Purchase Order for which Supplier has not begun to deliver the Services shall be deemed canceled, unless otherwise agreed in writing by the Company(ies) requesting or issuing such RFPs, proposals, and/or Purchase Orders, and (ii) this Agreement shall be terminated without liability or obligation to the Parties, except for any liabilities and obligations arising under any Purchase Orders issued by Customer or Company(ies) for which Supplier has already completed Services in accordance with the terms of this Agreement. 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 for which provision of Services has not been completed 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 issued by Customer or a Customer and for which Supplier has begun to deliver Services 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 Customer pursuant to the terms and conditions of such Purchase Orders.

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 Party at the address(es) specified in ***Schedule F*** attached to this Agreement and made a part hereof. 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 assignment or 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 the 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 the Customer 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.

[Signature page follows]

Avangrid Management Company, LLC

DocuSigned by:

4DEFD1FA35C6430...

Signature

Sergio Merchan

Print Name

CIO AVANGRID

Title

10/29/2021

[redacted]

Avangrid Management Company, LLC

DocuSigned by:

DEF09C2D80414A6...

Signature

Guillermo Fernandez

Print Name

Controller - Corporate Functions

Title

10/29/2021

SCHEDULES:

Schedule A: Companies
Schedule B: Services
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

Avangrid Renewables:
Avangrid Renewables LLC
1125 NW Couch St., Suite 700
Portland, OR 9720

SCHEDULE B

Services, Warranty, Deliverables, and Vendor Requirements

1. DESCRIPTION OF THE SERVICES

Partner should provide the following services:

- **Infrastructure Technical Services**: these services shall be provided for different technologies. The specific capabilities required for each technology are specified in the following sections
  - Central / Distributed Systems:
    - SAP Basis
    - X86 Platform, Windows, Linux systems
    - AIX Systems. UNIX, Suse
    - Storage
    - Database
    - Packages
  - End User Platform Technical Services

- **Networking & Communications Technical Services**
  - Telecommunications / Network Engineering
  - Network Security

The following sections contain a detail of their scope.

Any management activities that are required by the Partner to do the work properly will be responsibility of the Partner and considered as part of the service. Those activities that may be required to internally monitor and coordinate the contracted services that correspond to several related requests to ensure consistency of the solution, are part of the service at no additional cost for AVANGRID.

AVANGRID requires the Partner to manage the services being tendered through the tool specified by AVANGRID, to record, monitor, report, control and close Service Requests taking into account the process defined by AVANGRID for such a purpose. All service requests must be processed using that tool.

1.1 Infrastructure Technical Services

These services are oriented to provide specialized technical activities for infrastructure, covering Centralised and Distributed systems and End User Platform system:

- ***Central / Distributed systems*** – Data Center & Computer Room hosted and/or cloud base infrastructure consisting of enterprise server and storage systems plus regional file servers. The technical infrastructure services should cover the following main technology platform domains:

    - Wintel
    - UNIX (AIX) and Linux
    - SAP Basis
    - Packages
    - Storage
    - Database
    - Cloud

    The above technical infrastructure services also cover the platform manufacturer's virtualization platform based on HyV,VmWare, RHEV, and power VM and the Storage Area Networking and virtualization platforms defined in the following sections.

- ***End User systems*** – end user devices (desktop, laptop, thoughbook, tablets), office productivity, messaging and client application packaging. Services will cover also directory services infrastructure used across AVANGRID based on Microsoft Active Directory.

The activities to be covered by the Partner as part of the Infrastructure Technical Service are described below:

a) Perform key-contact role for specific technology domains or infrastructure platforms as assigned.
b) Perform Technical Infrastructure Design for key technology platforms as part of platform upgrade and refresh activities. This task also includes associated cost of ownership models for different design options.
c) Assist in the preparation of technical infrastructure standards including build and configuration standards for assigned technology domains.
d) Perform technical assessments/reviews between different infrastructure options as part of platform upgrade and refresh activities.
e) Provide monitoring operational support with incident analysis and resolution when required. Participate in the company infrastructure monitoring and provide Level 1 and Level 2 support when required.
f) Provide operational support to implement maintenance tasks associated to all the technological towers described before.
g) Supervise and in some instances perform software installation tasks as needed to assist project delivery. This activity is normally performed in conjunction with application vendors.
h) Perform capacity planning as part of technical platform role.

i) Provide technical input to architectural planning – utilizing relevant expertise to ensure that architectural plans and budgets reflect the activities and investment required to move from the current state to the desired state.

j) Provide installation, configuration and roll out of the hardware described before

k) Participate in Projects related with the technical towers described before as requested.

l) Support in their Procurement processes when required.

m) Plan and supervise changes to the systems, in accordance with IOC Change Management process, as required by operational or upgrade requirements

n) Some of services described before will be provided in a NERC-CIP Compliance environment. AVANGRID will work with the vendors to evaluate their NERC-CIP situation and cooperate on the resources certification process by adding them to the company existing structure, as required.

o) On-Call support over the services described before when required

p) Proactively seek the current processes and infrastructure improvement, through proposals to increase operational efficiency of the Avangrid systems and infrastructure, and/or simplifying the required infrastructure.

q) Participate in identifying and developing automation projects for recurrent manual tasks.

Infrastructure Technical Services shall be provided for different technologies. The specific capabilities required for each technology are specified in the following sections.

1.1.1 Infrastructure Technical Services – SAP Basis

For the SAP Basis Service, the following specific activities are required to be delivered by the Partner as part of the scope. The SAP Basis responsibilities include configuring, monitoring, tuning, and troubleshooting the SAP technical environment on an ongoing basis as well as scheduling and executing the SAP transport system.

- Installing and configuring all SAP systems and applications; installing patches / packages; Business Functions activation;
- Implementing OSS Notes:
- Backing up and restoring data;
- Tuning performance and troubleshooting problems;
- Managing batch jobs;
- Configuring SAP's transportation management system (TMS); managing transports;
- Running and managing background jobs;
- Setting up operation modes

Partner must provide a matrix showing their ability to provision resources with in-depth knowledge of these core technologies and provide supporting evidence.

SAP Platforms:

- SAP CRM 7.0. EHP4
- SAP ECC 6.0 (including SAP IS-U). EHP8
- SAP NWBC

- SAP Fiori
- SAP Transport Manager
- HANA 2.0
- SAP BW (non-HANA and HANA)
- SAP NW
- SAP CLM
- SAP GRC

1.1.2 Infrastructure Technical Services – X86 Platform

Partner must provide a matrix showing their ability to provision resources with in-depth knowledge of these core technologies and provide supporting evidence.

Hardware Platforms

- Dell, and HP Intel Hardware
- NUTANIX

Virtualization Platforms

- Microsoft Hyper-V
- VMWARE
- RHEV

Operating Systems

- Microsoft Windows 2012 onwards
- Red Hat Linux

Directory Services

- Microsoft Active Directory

Containers:

- OpenShift

1.1.3 Infrastructure Technical Services – Packages

Partner must provide a matrix showing their ability to provision resources with in-depth knowledge of these core technologies and provide supporting evidence.

Packages:

- IBM FileNet. ICN, Full and Cache systems. DMZ Implementations
- IBM FileNet Storage
- IBM Case Manager
- TripWire Configuration control manager
- Logging Systems (logInsight, Splunk, LogRythm)
- MS Sharepoint 2016 / 2010
- BMC Control-M

- Automic (UC4)
- Autosys
- Crowdstrike
- CyberArk PAM
- ANSIBLE
- Elastic
- Satellite
- SCCM

Applications Servers

- Java Application Server (JBOSS)
- Websphere Application Server

1.1.4 Infrastructure Technical Services – AIX Systems

Partner must provide a matrix showing their ability to provision resources with in-depth knowledge of these core technologies and provide supporting evidence.

Hardware Platforms

- IBM Hardware
- IBM p-series hardware

Operating Systems

- UNIX (AIX v6.x)
- Redhat Linux v6.x
- Linux CentOS, SUSE

1.1.5 Infrastructure Technical Services – Database

Partner must provide a matrix showing their ability to provision resources with in-depth knowledge of these core technologies and provide supporting evidence.

Hardware Platforms

- Oracle, SQL and DB2 database platforms

Databases

- Oracle 19
- Oracle RAC
- SQL Server 2008 onwards
- SAP Hana 2.0
- PostgreSQL

1.1.6 Infrastructure Technical Services – Storage

Partner must provide a matrix showing their ability to provision resources with in-depth knowledge of these core technologies and provide supporting evidence.

Hardware Platforms

- IBM SVC
- IBM & NETAPP & EMC Storage Arrays
- EMC Data Domain

Systems Management Platforms

- IBM Tivoli Storage Manager
- Symantec BackupExec
- HP Arcsight
- Veeam backup and DR Orchestrator
- Enterprise Vault and backup
- Commvault backup

1.1.7 Infrastructure Technical Services – End User Platforms

End user devices (desktops, laptops, thoughbooks, tablets), office productivity, messaging and client application packaging. Services will cover also directory services infrastructure used across AVANGRID based on Microsoft Active Directory.

Partner must provide a matrix showing their ability to provision resources with in-depth knowledge of these core technologies and provide supporting evidence.

Hardware Platforms

- DELL, HP Hardware for Desktops and Laptops
- DELL, Panasonic Hardware for thoughbooks
- Android Mobile devices

Apps Virtualization

- XenApp, Citrix
- Flexxible

Mobility

- Intune

Patching and packaging

- Altiris
- MSI

Messaging / Collaboration Platform Services

- O365
- Jabber

1.1.8 Infrastructure Technical Services – Cloud

Partner must provide a matrix showing their ability to provision resources with in-depth knowledge of these core technologies and provide supporting evidence.

Cloud Technologies

- Azure, AWS, Google

Cloud Systems

- IAAS , VM, Storage, database, networking, AKS,
- PAAS

Cloud Governance

- Operational model, change management
- Cost model

1.1.9 Infrastructure Technical Services – Operations

Partner must provide a matrix showing their ability to provision resources with in-depth knowledge of these core technologies and provide supporting evidence.

Change Management

- Service modelling
- Service management
- Service Now
- Asset Management, CMDB Automation

Operation Support

- Incident Management
- Problem Management
- Notification system
- Cloud operations

Monitoring

- BMC Patrol
- Entuity
- AppDynamics
- Cloud monitoring

DataCenter

- DCIM
- DC engineering

1.2 Networking & Communications Technical Services

These services are oriented to provide specialized technical activities to cover Local and Wide Area Networks, mobile networks and associated networking components such as load balancers, firewalls and proxy servers.

The activities to be covered by the Partner as part of the Networking & Communications Technical Services are described below:

a) Perform key-contact role for specific networking technology domains assigned.

b) Perform Network Infrastructure Design for key platforms as part of upgrade and refresh activities. This task also includes associated cost of ownership models for different design options.

c) Assist with network design of solutions within the relevant domain, ensuring compliance with Group standards and direction.

d) Develop business cases that define the costs, benefits and delivery approach for a network project, leading to approval for project delivery.

e) Perform supplier management covering various networking-telecomm suppliers and supervising the delivery of network and communication services from them.

f) Assist technical support staff as required with the resolution of escalated operational problems and restoration of service to customers.

g) Plan and supervise changes to the network, in accordance with AVANGRID IT IOC Change Management process, as required by operational or upgrade requirements.

h) Assist with capacity planning on AVANGRID's LAN/WAN network ensuring all known factors affecting future performance are addressed through plans for upgrades, enhancements, etc.

i) Provide technical input to network planning and forecasting activities.

j) Provide technical support for network procurement activities to ensure that products or services being procured meet the required technical standards and specifications.

k) Perform network technical assessments/reviews between different networking infrastructure options as part of platform upgrade and refresh activities.

l) Provide technical input to network planning utilising relevant expertise to ensure that network plans and budgets reflect the activities and investment required to move from the current state to the desired state.

m) Perform key-contact role for specific technology domains or infrastructure platforms as assigned.

n) Perform Technical Infrastructure Design for key technology platforms as part of platform upgrade and refresh activities. This task also includes associated cost of ownership models for different design options.

o) Assist in the preparation of technical infrastructure standards including build and configuration standards for assigned technology domains.

p) Perform technical assessments/reviews between different infrastructure options as part of platform upgrade and refresh activities.

q) Provide monitoring operational support with incident analysis and resolution when required. Participate in the company infrastructure monitoring and provide Level 1 and Level 2 support when required.

r) Some of services described before will be provided in a NERC-CIP Compliance environment. AVANGRID will work with the vendors to evaluate their NERC-CIP situation and cooperate on the resources certification process by adding them to the company existing structure, as required.

s) On-Call support when required

The specific technical capabilities required from the Partner for these Networking & Communications Technical Services are specified in the following sections.

1.2.1 Infrastructure Technical Services – Telecommunications Network Engineer

Partner must provide a matrix showing their ability to provision resources with in-depth knowledge of these core technologies and provide supporting evidence.

Networking

- Cisco Switches
- Cisco Routers
- Network Management Systems (Cisco DNA, Cisco Live Action)
- Networking Software (IOS, NX-OS)
- CISCO NAC Systems
- SDN, SD-WAN
- Netscaler Load Balancers

Wide Area Networks

- Transmission media: Ethernet, LTE/5G, Satellite, Mobile Services, Broadband.
- Transmission infrastructure: optical fibre, radio links, microwaves
- Backbone: MPLS, VPN
- Transport: DMVPN, SD-WAN (Cisco I-WAN)

Mobility & Wireless

- Indoor Access Points

- Outdoor and Industrial Access Points
- CISCO Wireless LAN Controllers

Telephony & VoIP

- Cisco VoIP Architecture
- Unified communications
- SIP Trunk Infrastructure

1.2.2 Infrastructure Technical Services – Network Security

Partner must provide a matrix showing their ability to provision resources with in-depth knowledge of these core technologies and provide supporting evidence.

Security Internet / DMZ

- Network Security
- Services and Endpoint security
- Firewalls-IPS Products: Checkpoint, CISCO, Palo Alto
- Bluecoat Proxy Servers
- SSL Decryption
- DNS InfoBlox
- DdoS Radware

2. OPERATIONAL MODEL

This chapter describes a high-level view of the operation of the service. It describes the processes and operational tasks for the service, and the associated deliverables and establishes the interactions between AVANGRID and the Partner to carry out the work under the service contract.

2.1 General view

Partner will deliver the service in accordance with AVANGRID quality standards.

AVANGRID will provide the requirements and scope of the work to be performed and will request the service (service work-package) to Partner.

Partner will analyze the service request and provide a detailed effort evaluation for the service work-package delivery.

AVANGRID will analyze the proposal received, accept and assign the service to the Partner.

Partner will start the work according with the evaluation agreed. Quality checks will take place during this stage.

2.2 Changing Scope Elements

The service can incorporate new technologies during the term of the contract. It is essential for AVANGRID that changes on technologies are accompanied by variations in the necessary services, in the sense of maintaining the SLAs in place, as well as to improve service management efficiency.

Partner must be capable of adapting services to incorporate any technological changes that may arise from the evolution, replacement or adding new technologies and platforms.

Technologies can evolve or be replaced during the term of the Contract. Any new technology replacement or addition will be part of the scope of the Service and will not impact on the agreed contract price.

The following schema must be used to incorporate new development technologies:

- AVANGRID will decide and inform Partner of the technology to be incorporated into the service. Partner must define an incorporation plan specifying the time required and the new SLAs based on what is requested by AVANGRID. The incorporation plan must contain an estimate of the impact on maintenance activities.

- AVANGRID will decide the retirement of technologies, whether for strategic reasons or technological obsolescence. Partner must submit a report with an estimate of the impact on maintenance activities.

2.3 Capacity Management

AVANGRID will anticipate as earlier as possible the capacity that will be needed by the Partner so that the Partner can ensure the adequate availability of resources to meet AVANGRID needs.

AVANGRID requires that the Partner must provide the necessary resources within a period of less than **2 weeks** from the service work-package assignment (service request). Partner must describe / propose the mechanisms that allow him to ensure this availability.

On a **yearly** basis AVANGRID will send the Partner its best estimate of its needs for the whole year. This information will be based on the annual project portfolio and must be understood as a preliminary approach, without committing AVANGRID in any way as to its delivery, compliance or accuracy.

Partner will continuously monitor the demand received with the aim of adapting its capacity to this demand.

2.4 Knowledge Management and Retention

2.4.1 Knowledge management

Partner will compile, document, manage and use the knowledge acquired. Especially, knowledge related to the resolution of requests, request types, contingency solutions and the procedures related to the operating and running of the service. This commitment applies particularly to the knowledge related to the design and building of solutions and the procedures specific to the operation and execution of the service.

Knowledge Management main objective is to create a service-knowledge map and encourage learning and continuous improvement.

All the knowledge bases used and generated when providing the service shall be owned solely and exclusively by AVANGRID. If this information is generated on a tool belonging to the Partner, the mechanisms required to extract the information and deliver it to AVANGRID in a compatible format must be defined

Likewise, any document generated by the Partner during the provision of the service shall also be owned solely and exclusively by AVANGRID and must be versioned, stored, distributed and managed as any other type of knowledge asset generated during provision of the service.

All the knowledge assets used and generated when providing the service must be considered property of AVANGRID. If this information is generated on a tool belonging to the Partner, it will implement the mechanisms required to extract the information and deliver it to AVANGRID in a usable format

Partner will define training plans to improve the ability of the work team to provide the service. Partner must specify the training action proposals their employees will receive to provide the service and the content and duration of such training.

Knowledge management plan must have actions to manage rotations in the service team to avoid any loss of knowledge and thus mitigate the risks such rotations might represent when providing the service. If the Partner decides to replace personnel assigned to service tasks, there must be an overlap period to ensure the adequate transfer of knowledge and keep the service quality.

2.4.2 Knowledge Retention

Partner will commit to permanently maintaining throughout the term of the contract a work team with enough members and with the right quality to comply with the SLAs and with the quality required by the technical specifications.

Partner must ensure a quick and adequate knowledge transfer of the service to any new resources that may be assigned to its provision, without this assignment jeopardising the committed SLAs or involving any effort or additional cost for AVANGRID.

Partner must ensure the adequate knowledge transfer of the service between the outgoing and incoming resource. Knowledge transfer must be accomplished at no additional cost to AVANGRID.

3. SERVICE STAGES

Following service stages will be provided by the Partner to ensure quality provision as well as to return the service with guarantees:

- ***Regular Service Provision Stage***.
- ***Service Return Stage.***

3.1 Regular Service Provision

The regular service provision stage will begin with the assignment by AVANGRID, of the service request to the Partner.

During this stage, the mechanisms described below must be followed:

- The service operating model defined by AVANGRID must be applied;
- The service levels will apply in this period. All metrics and indicators will be calculated in this period and the corresponding reports generated;
- Partner will invoice according with the service economic model.

3.2 Service Return

The service will be returned for any of the following reasons:

- Termination of the contract due to finalization of the agreed contractual period;
- Early contract termination;
- Significant non-compliance with the SLAs established herein for ***six (6) consecutive months*** from the start of the provision of the regular service.

The objective is to guarantee effective transfer of all knowledge and/or acquired/generated assets during service provision. Return will be made to AVANGRID or to any other provider that AVANGRID identifies.

If the contract is rescinded for those reasons stipulated, the Partner must return control of the service under contract, define a detailed Return Plan and lead its execution while actively collaborating with AVANGRID or the appointed provider.

Partner will carry out the return work in parallel with the normal service provision, without any relaxation or elimination of the quality commitments stipulated in the SLAs and **without any additional cost** to AVANGRID.

Partner must take no more than ***three (3) months*** to complete the return stage. This stage will consist of two main phases, planning and return execution, which are described below.

The Partner will assign the adequate professional profiles at any given time to carry out the return, and should indicate in the proposal the **minimum of hours of work** for the execution of this stage and at **no additional cost** to AVANGRID.

If the return effort proves to be insufficient because the SLAs are subject to a noticeable deterioration as a result of the return stage or for any other reason, both parties agreed to extend the return of service stage for as long as AVANGRID requires.

Partner is responsible for the extension in terms of planning and duration. The possible additional cost for extending the maximum return period established will be billed at the current regular service price.

No costs will be charged for any travel to AVANGRID's facilities that may be required for the return of the service.
Partner will provide post-return support if so requested by AVANGRID under the following terms and conditions:

- Resources that have participated in the previous stages of the return process are (mainly) required for this support. Any such services will be billed on the basis of the dedicated hours at the current regular service price.
- It is estimated that any post-return service support will last for **three (3) months**.

3.2.1 Planning Execution

Partner must include the preparation and delivery of the service return plan. Once the return stage has started, the Partner has no more than ***one (1) week*** to deliver the return service plan that must be approved by AVANGRID. At a minimum, the plan must cover the following aspects:

- Breakdown of phases, sub-phases and deliverables required to correctly transfer the service;
- Provide updated documentation in relation to the services provided;
- Up-to-date inventory of logical, documentary and physical assets that must be taken into account during the transfer. This must also include physical assets owned by the Partner that could be transferred to AVANGRID or the newly appointed provider;
- In relation to assets transferred to the Partner by AVANGRID to provide the service, the Partner must return these assets in perfect condition once the provision of the service has ended;
- Notify any existing problems and potential risks in the service that could jeopardise the correct return of the service;
- Assign a sufficient work team with the key resources to ensure success during the return stage.

3.2.2 Returning the Service

Partner must actively collaborate with AVANGRID and the newly appointed provider during the return stage. This stage covers all those activities required by the Partner to ensure that the AVANGRID services in question are properly kept up and running during the transfer of service and to facilitate the transfer of the services over the newly appointed provider.

This stage involves at least the following phases and activities:

- **Training**: Partner is responsible for adequately training the new provider team according to its profile, as well as for carrying out simulation runs and reviewing the results;
- **Documentation**: Partner is responsible for identifying and compiling all the information required to enable the incoming provider to provide the service properly;
- **Taking control**: objective is to gradually transfer the service to the new team in an orderly manner, gradually reducing the presence of Partner team members;

- **Certification**: objective is to monitor the evolution of the SLAs during the process and establishing the corrective actions to maintain the SLAs;
- **Post-completion**: access to key service managers to make enquiries for at least three **(3) months** after the completion of the return stage.

4. GOVERNANCE MODEL

The Governance Model proposed is structured bilaterally between AVANGRID and the Partner. The schedule to hold these Committees will be agreed at the start of the service. The minimum structure of committees proposed for proper service governance is described below.

4.1 Steering Committee

Objectives:

- To present medium-term plans and planned projects;
- To provide a global evaluation of the provision of the service;
- To approve the Quality Plans submitted;
- To manage Operations Committee scaling actions;
- To ensure that the service provided is aligned with AVANGRID strategic initiatives and objectives;
- To define and change the guidelines and principles to provide the service. To propose amendments to the service contract;

Frequency: the meeting will be held every 6 months and/or further ones can be organized as requested by AVANGRID or the Partner.

The Partner must deliver/agree with AVANGRID a status report for the corresponding review period which will be managed during the meeting. This report must be prepared sufficiently in advance of the meeting.

4.2 Operations Committee

Objectives:

- To globally monitor the service and manage contract clauses to ensure proper application;
- To monitor how service provision operates;
- To resolve extraordinary problems;
- To monitor compliance with Service Level Agreements and to propose corrective measures in the event of breaches;
- To analyze and manage risks and provide solutions;
- To monitor the estimated and real capacity executed;
- To ensure compliance with and report on any agreements entered into.

Frequency: this committee will meet once a month.

The Partner must deliver/agree with AVANGRID a status report for the corresponding review period which will be managed during the meeting. This report must be prepared sufficiently in advance of the meeting.

4.3 Technical Meetings

Activities: these meetings will deal with specific technological area and service needs (working groups, technologies, etc.). The objective is to deal with specific problems that affect particular projects.

Frequency: the frequency of these technical meetings will depend on the specific needs of each project and situation.

5. SERVICE LEVEL AGREEMENTS (SLAs)

The purpose of the Service Level Agreement (SLA) is to establish an objective framework to measure compliance with the service level required by AVANGRID for the service under this contract.

A group of SLAs have been defined that will be used to evaluate the quality of the service received. AVANGRID will be in charge of measuring, compiling the information and calculating the indicators.

Service quality will be understood as compliance with the different Service Level Agreement requirements for the service. A specific target and minimum satisfaction level will be defined SLA. Non-compliance with the target values will involve penalties.

The following table contains the KPIs defined by AVANGRID, to control the provision of the service and measure its compliance.

KPI	Description	Target SLA	Penalty
Service Request Evaluation Delivery Date	% of Service Requests whose effort evaluation has been provided in less than 5 working days.	>= 90%	1%
Service Request Start Date	% of Services Requests started in less than 10 working days, after service request assigned	>= 90%	2%
Documentation errors	% of service request delivered with errors o lack of documentation as part of the quality standard procedure as defined by AVANGRID.	<5%	1%
Customer Satisfaction	Achieve Customer satisfaction score from AVANGRID IT IOC Managers	> 85%	1%
Resources availability	Number of additional days where the needed resources to deliver the service are not available after 10 working of the service assignment	< 5 days	2%

Indicators will be reviewed regularly to determine the level of evolution required:

- Alignment with new AVANGRID business needs;
- Constant improvement of target levels;
- Reiterated non-compliance with the minimum level (this situation can be lead to service non-compliance and, therefore, breach of contract).

SLAs will be measured every **three (3) months**. In case of non-compliance with the SLA, a specific amount of free hours of service will be generated, which AVANGRID can execute to perform the tasks / projects it deems appropriate. This specific amount of free hours will be calculated in the following way:

- The amount of free hours is calculated as the percentage of the total service hours executed by the Partner in the three months period where SLAs are measured.
- Each SLA has an assigned penalty percentage.
- In case of not compliancy of the SLA, the penalty percentage will be applied to the total service hours delivered by the Partner during the three months period.
- In case of non-compliance of several ANSs, the percentages would be added until reaching a **maximum value of 15%** of the total service hours in the six months period.

If there are no requests for a corresponding indicator, a zero (0) penalty value will be assumed.

Penalties for SLA non-compliance will apply without prejudice to the obligation of the Partner to compensate for the damage such non-compliances might cause AVANGRID.

6. SERVICE ORGANIZATION

AVANGRID requires bidding companies structure the service delivery organization in the best possible way to provide the service in accordance with the technical scope and quality indicators committed.

Partner should provide a clear roles and profiles description of the service organization model, including the Curriculum Vitae of the professional profiles that will deliver the service, indicating for each of them the role they will play within the service.

Partner must make an organisation proposal that includes, at least, the following roles and responsibilities.

Two different Service profiles will be required for each role:

- **Specialist**: 2 - 8 years of experience in the technical area of expertise in a number of large clients similar in size to AVANGRID. Depth technical experience covering the required technology domains. Experience of customer and supplier management.

- **Senior Specialist**: > 8 years of experience in the technical area of expertise in a number of large clients similar in size to AVANGRID. Depth technical experience covering the required technology domains. Experience of customer and supplier management.

Role	Activities / Responsibilities
Infrastructure Technical Specialist – OS (Windows, Linux and Unix)	• Intel Platforms (Enterprise class including Blade Chassis and servers) • Virtualisation platforms (specification, design and build) covering Microsoft Hyper-V, VMWARE, and RED HAT Virtualization (RHEV). • MS Virtual Machine Manager • Specification, Design and Administration of Windows 2012 and SQL Server 2012 onward. • Specification, Design and Administration of Linux platforms covering Redhat Linux v8.3 onwards. • Scripting and automation through Powershell, Playbooks... • MS Active Directory design and administration • Containers, RedHat Openshift • Windows Networking design and configuration • IIS Web, application server and database design • Apache Web, IBM Websphere Application Server, JBOSS Application Server • Windows performance analysis and tuning • Configuration Management • Systems management including backup and monitoring • Disaster Recovery • IBM p-Series and Oracle Solaris platforms • Virtualisation platforms (specification, design and build) covering IBM Logical Partitions (LPAR), live partition mobility and IBM San Volume Controller • Specification, Design and Administration of IBM p-Series covering AIX 7.x and Solaris 10 onwards. • SuSe • Shell scripting • UNIX / Linux LDAP integration (MS Active Directory) • UNIX / Linux Networking design and configuration • DBA exposure (such as Oracle / MySQL database architecture, design, administration and installation) • UNIX / Linux performance analysis and tuning • Systems management including backup and monitoring

Role	Activities / Responsibilities
Infrastructure Technical Specialist - Packages	• IBM Filenet • IBM Case Manager • IBM Mobile Apps Filenet Integration • Sharepoint environment • BMC Control-M • Automic (UC4) • Autosys • Crowdstrike • CyberArk PAM • Ansible Tower • Elastic Search • Satellite • SCCM
Infrastructure Technical Specialist – SAP Basis	• SAP CRM 7.0. EHP4 • SAP ECC 6.0 (including SAP IS-U). EHP8 • SAP NWBC • SAP NW • SAP Fiori • SAP Transport Manager • SAP BW (non-HANA and HANA) • SAP CLM • SAP GRC
Infrastructure Technical Specialist - Database	• Oracle, SQL and DB2 database platforms • Oracle 12c onwards • Exadata • SQL Server 2008R2 onwards • SAP Hana 2.0 • PostgreSQL
Infrastructure Technical Specialist - Storage	• IBM San Volume Controller • IBM & NETAPP & EMC Storage Arrays • DELL Data Domain • Commvault • Data replication

Role	Activities / Responsibilities
	• HP Arcsight • DR Orchestrator • Enterprise Vault and backup
End User Platform Specialist	• Desktop, laptop and tablet platforms • Microsoft Windows 10 • Microsoft file sharing platforms • Windows desktop scripting languages (such as PowerShell) • MS Active Directory administration • Desktop networking configuration • Desktop software packaging and testing • MS Office and MS Outlook / O365 setup and configuration • Desktop imaging and deployment • Experience with applications virtualization: Citrix and Flexxible environments • Experience with cloud application virtualization • Experience with virtualization solutions to support DR / Business Continuity

Role	Activities / Responsibilities
Telecomm Specialist	• Network design covering wired and wireless networks • Network Capacity management • Network support • Cisco Switches, Routers • Network Management Systems (Cisco DNA, Cisco Live Action) • Networking Software (IOS, NX-OS) • CISCO NAC Systems • CISCO SDN • Transmission media: Ethernet, LTE/5G, Broadband, Satellite, Mobile Services • Transmission infrastructure : optical fibre, radiolinks, microwaves • Backbone: MPLS, VPN • Transport: DMVPN, SD-WAN (Cisco I-WAN) • Indoor Access Points • Outdoor and Industrial Access Points • CISCO Wireless LAN Controllers • Cisco VoIP Architecture • Unified communications • SIP Trunk Infrastructure
Network Security Specialist	• Network Security Design • Services and Endpoint security • Firewalls-IPS Products: Checkpoint, CISCO, Palo Alto • Netscaler Load Balancers • Bluecoat Proxy Servers • SSL Decryption • DNS InfoBlox • DdoS Radware
Cloud Specialist	• Azure, AWS, Google • IAAS , VM, Storage, database, networking, AKS, • PAAS • Operational model, change management • Cost model

Role	Activities / Responsibilities
Specialist Operation	• Service modelling • Service management • Service Now • Asset Management, CMDB Automation • Incident Management • Problem Management • Notification system • Cloud operations • BMC Patrol • Entuity • AppDynamics • Cloud monitoring • DCIM • DC engineering

Service costs

The price model that applies to the provision of this service will be based on a ***price per hour,*** for the different services:

Infrastructure Technical Services	Price/hour ($/h)
SAP Basis	
Infrastructure Technical Specialist	
Senior Infrastructure Technical Specialist	
X86. Windows Linux	
Infrastructure Technical Specialist	
Senior Infrastructure Technical Specialist	
AIX - Unix	
Infrastructure Technical Specialist	
Senior Infrastructure Technical Specialist	
Packages	
Infrastructure Technical Specialist	
Senior Infrastructure Technical Specialist	
Storage	
Infrastructure Technical Specialist	
Senior Infrastructure Technical Specialist	
Database	
Infrastructure Technical Specialist	
Senior Infrastructure Technical Specialist	
End User Platform	
Infrastructure Technical Specialist	
Senior Infrastructure Technical Specialist	
Operations	
Infrastructure Technical Specialist	
Senior Infrastructure Technical Specialist	

Networking and Communications Technical Services	Price/hour ($/h)
Networking	
Networking and Communications Specialist	
Senior Networking and Communications Specialist	

Prices for the services must cover all the activities related to the service, as described in this document. **As noted in Schedule D**

The cost of the service must include all the costs derived from it. This cost must include the cost of all those specific tools or products that the Partner proposes to use for the realization of the service, being the responsibility of the Partner any management derived from the use of that tools.

The costs of management / governance of the service, administration, coverage for sick leave, holidays, training.., will be considered as included in the unit cost provided.

AVANGRID will anticipate to the Partner the service plan in advance as soon as possible so that it can adequately respond to the needs of AVANGRID. This service plan will be forecast and will not be a commitment from AVANGRID.

No travel expenses will be considered within USA territory unless fully required for the service delivery and upon AVANGRID agreement. Travel costs will be managed case by case.

Travel Expenses

Travel expenses arising from the provision of the service under the terms and conditions stipulated in this document, as well as those arising from training and the transfer of knowledge of the applications will be part of the service at no additional cost for AVANGRID.

No travel expenses will be considered within USA territory unless fully required for the service delivery and upon AVANGRID agreement. Travel costs will be managed case by case.

All travel expenses must be clearly explained and will be reviewed and approved beforehand by AVANGRID.

Invoicing model

Partner should issue one invoice to AVANGRID to be paid for the services delivered. Each of the services delivered must be detailed in the invoice. Resource Types

SERVICE PHASES

The following service stages are required to ensure quality provision as well as to return the service with guarantees:

- ***Service Transfer Stage***, to transfer / acquire the service;
- ***Regular Service Provision Stage***;
- ***Service Return Stage***, which consists of returning the service to AVANGRID or a third party designed by AVANGRID upon termination of the contract.

SERVICE TRANSFER (Service acquisition)

The incoming provider will be in charge of acquiring the service. This stage will conclude on the incoming provider assuming responsibility for the service.

The transition/acquisition stage is considered from notification of the final award to the acceptance of the transfer milestone.

The bidding company must submit a transfer plan to acquire the service no later than ***one (1) week*** as of the notification of the final award of the service. ***Two (2) months*** is the maximum time for the transfer stage. Nonetheless, AVANGRID would be interested in the transition stage being completed in the shortest possible time.
It is recommended to be followed a schema based in application blocks that consists of at least the following steps:

- Service transfer planning stage;
- Service transfer development stage;
- Service transfer responsibility milestone.

AVANGRID requires the provider to execute the following activities during the transition stage:

- Setting up a specific committee to monitor the transition;
- Creation of several service governance and monitoring committees;
- Planning the incorporation of new work teams;
- Starting up of operating procedures;
- Adopting of management tools;
- Reviewing existing documentation on the applications and identifying possible gaps;
- Implementing the knowledge management system;
- Documenting all activities carried out during the transition.

During the **two (2) months** of the transfer stage a review, implementation and measurement of the SLAs will be made to check the degree of compliance with the SLAs and to evaluate if the service can be transferred to the provider with enough guarantees to meet the required quality before the milestone of service transfer responsibility.
In this period, the providers cannot be penalised with respect to SLAs, but a decision will be made as if the service transfer milestone can be accomplished with sufficient guarantees.

Service Transfer Planning

Planning will be based on the transfer plan defined by the incoming provider, which can be completed with the exit plan proposed by the outgoing provider. In this planning stage, the incoming provider will assume any costs it may incur.
At least the following objectives must be met in this period:

- Review of the service transfer schedule. AVANGRID may change the start date, duration and content of each one of the stages, where necessary, to ensure achievement of full service transfer within the desired terms and conditions.
- Review of the knowledge transfer schedule of the processes and tools required to provide the service, as well as to implement all the mechanisms, responsibilities and tools associated with AVANGRID supervision model.
- Identification and analysis by the provider of all the logistics involved in providing the service, as well as a risk analysis that might be associated with taking over control of the service and the corresponding mitigation and contingency plan.
- AVANGRID requires that the transfer plan submitted contain at least the following:
    - Detailed planning of knowledge transfer activities, containing:
        - Specific and formal training of the provider team. If the incoming provider requires training from the outgoing provider, it will be responsible for agreeing the conditions, at no additional cost for AVANGRID.
        - Required documentation. The provider is responsible for identifying and compiling all the information required to provide the service properly. When there is no previous documentation, the provider must plan and prepare it, at no additional cost for AVANGRID.
    - Planning the transfer milestone, indicating the sequence of activities to be done to take effective control of the service.
    - Identification of dependencies between applications.
    - Planning the incorporation of resources.
- Transition risk plan, containing the main risks and associated actions, especially focusing on the continuity of maintenance activities and projects currently in progress.

Provider must include in the proposal the required resources dedication, both from the incoming provider as well as the outgoing provider, along with the required documentation.

Service Transfer Execution

The objective of this stage is to execute all the activities required to enable the incoming provider to meet AVANGRID requisites.

All the activities required to be done at this stage will not have any cost to AVANGRID.
Provider can invoice the production hours as of the effective moment in which the service is transferred i.e. as of compliance with the transfer milestone of service responsibility, as described below.

Service Transfer Responsibility Milestone

Service transfer is completed with the transfer milestone that AVANGRID must approve. After that, the new provider will be fully responsible for the service, thus being the beginning of the regular service provision stage. This will be the moment at which the incoming provider will be able to invoice for the services being provided to AVANGRID.

Before completing the transfer of each application, AVANGRID will conduct the formal validations. If the incoming provider cannot take the responsibility for the service on the agreed dates in the transition plan or does not reach the required level of capability/quality to acquire the service, the incoming provider must subcontract to the outgoing provider until the validation is passed. If this situation lasts for long, for all or part of the services covered by the current service contract, AVANGRID will have the right to rescind the contract with the incoming provider.

Regular Service Provision

The regular service provision stage will kick off with the approval of the responsibility service transfer milestone by AVANGRID.
Once the provider has acquired the service, the mechanisms described below must be followed:

- The provider is responsible for the service under contract;
- The service operating model defined by AVANGRID must be applied;
- The complete scope of service levels will apply in this period. All metrics and indicators will be calculated in this period and the corresponding reports generated;
- As the provider is responsible for the service in this period, the provider will be authorised to begin invoicing according with the service economic model.

SERVICE RETURN

The service must be returned for any of the following reasons:

- Termination of the contract due to finalization of the agreed contractual period;
- Early contract termination;
- Failure to comply with the service transfer stage under the terms and conditions stipulated;
- Significant non-compliance with the SLAs established herein for ***three (3) consecutive months*** from the start of the provision of the regular service (and after the finalization of the stabilisation period).

The objective is to guarantee effective transfer of all knowledge and/or acquired/generated assets during service provision. Return will be made to AVANGRID or to any other provider that AVANGRID defines.
If the contract is rescinded for those reasons stipulated, the provider must return control of the service under contract, define a detailed Return Plan and lead its execution while actively collaborating with AVANGRID or the appointed provider.

Return work must be undertaken in parallel to normal service provision, thus no service quality commitments stipulated in the SLAs can be impacted. Furthermore, return work will involve no additional cost for AVANGRID.

Provider must take no longer than ***three (3) months*** to complete the return stage. This stage will consist of two main phases, planning and return execution, which are described below.

Provider assumes a commitment to assigning the appropriate professional profiles to undertake the return process at any moment, including all the Management roles. ***Provider should include as part of the proposal an estimated minimum effort of return hours for each technology block, at no cost for AVANGRID, including all the Management roles***.

If cases the SLAs are being subject to a noticeable deterioration as a result of the return stage, the return service stage can be extended as long as AVANGRID requires. The additional cost that may be involved in extending the maximum return period established will be invoiced at the regular service price.

Planning Execution

Provider must include the preparation and delivery of the service return plan. Once the return stage has started, the provider has no later than ***one (1) week*** to deliver the return service plan that must be approved by AVANGRID. The plan must cover the following aspects at least:

- Breakdown of phases, sub-phases and deliverables required to correctly transfer the service;
- Provide updated documentation in relation to the services provided;
- Up-to-date inventory of logical, documentary and physical assets that must be taken into account during the transfer. This must also include physical assets owned by the provider that could be transferred to AVANGRID or the newly appointed provider;
- In relation to assets transferred to the provider by AVANGRID to provide the service, the provider must return these assets in perfect condition once the provision of the service has ended;
- Notify any existing problems and potential risks in the service that could jeopardise the correct return of the service;
- Assign a sufficient work team with the key resources to ensure success during the return stage.

Returning the Service

Provider must actively collaborate with AVANGRID and the newly appointed provider during the return stage. This stage covers all those activities required by the provider to ensure that the AVANGRID services in question are properly kept up and running during the transfer of service and to facilitate the transfer of the services over the newly appointed provider.
This stage involves at least the following phases and activities:

- **Training**: provider is responsible for adequately training the new provider team according to its profile, as well as for carrying out simulation runs and reviewing the results;
- **Documentation**: provider is responsible for identifying and compiling all the information required to enable the incoming provider to provide the service properly;

- **Taking control**: objective is to gradually transfer the service to the new team in an orderly manner, gradually reducing the presence of provider team members;
- **Certification**: objective is to monitor the evolution of the SLAs during the process and establishing the corrective actions to maintain the SLAs;
- **Post-completion**: access to key service managers to make enquiries for at least **two (2) months** after the completion of the return stage.

SUBCONTRACTING

Bidders shall be capable to provide all services specified in this tender with their own resources. However, under specific circumstances bidders can create partnerships with other vendors and subcontract part of the services stipulated in this tender.

The circumstances will be driven by the achievement of better transformation, technical and economic solutions to AVANGRID without putting in risk the service quality. Exceptions will be clearly defined and justified under the factors described before.

AVANGRID will have the right to authorize the partner to subcontract part of the services to other service providers.
Bidders shall indicate:

- Locations where partnerships are required
- Partners and the level of partnership (long-term relationship or partnership)
- Highlight limitations or constraints of the service due to a partnership (including impact on end-to-end traffic flow differentiation).

Partner awarded with the service will be the prime contractor and the only responsible of the contract terms and conditions compliancy and service delivery.

SERVICE CONDITIONS

Service Duration

This is a ***3-year*** term contract. AVANGRID may terminate the contract early and unilaterally, solely being obliged to settle the amounts payable up to the time of early termination, as long as the Partner is notified no later than **three (3) months** before the effective termination. Once this prior notice of contract termination has been done, Partner must continue providing the service, taking any necessary steps to ensure that effective service provision during the transition period is guaranteed.

The service must be returned for any of the following reasons:

- Termination of the contract due to completion of the agreed contractual period;
- Early contract termination;
- Significant non-compliance with the SLAs established herein for **six (6) consecutive months** from the start of the provision of the regular service.

Partner must collaborate with AVANGRID in defining and executing a return service plan that makes it possible for AVANGRID or a third party appointed by AVANGRID to take over the service under optimum conditions by means of a transfer of the assets, knowledge and information related to the service.

Location of the service

Service will be provided **on-shore** in AVANGRID facilities in the USA territory:

- Rochester – NY
- Augusta – ME
- Orange – CT
- Portland – OR

AVANGRID has a number of business critical platforms in various data centers, operations centers and generations sites.

Remote work may be considered under special circumstances.

Partner should note that assigned resources may be required to travel for project specific issues to participate in workshops, project and design meetings.

In some cases, resources may be required to work in remote locations for short periods of time.

Service hours

Service provision working hours to manage AVANGRID service requests are from **7:30AM to 4:30PM USA East and West Time,** depending on the location of the resources, from Monday to Friday.

AVANGRID could require that the Partner deliver some support services outside the normal service hours, in specific operations support activities. These extraordinary situations will be agreed between the Partner and the requestor depending on the needs of each project.

Services Provisioning Capability

a) Partner will have the resources with the necessary training and experience for delivering the Service and to ensure ongoing and refresher training in the terms necessary for the correct provision of the Services, considering the necessary professional profiles, technical and functional knowledge, etc.

b) All personnel through which the Partner will carry out the work will, to all effects, be under the exclusive liability of the Partner, who thus assumes with respect thereto the legal character of employer, including all the inherent rights and obligations that such a condition brings therewith, in full compliance at all times with current labour and company legislation so that its employees may not be considered de facto or de jure employees of AVANGRID.

c) Particularly, the Partner will comply punctually with the payment of salaries and Social Security contributions of its personnel involved in the performance of same, as well as to deposit the withholding tax of these employees for income tax purposes at the tax office.

d) Annually and whenever requested to do so by AVANGRID, Partner shall provide AVANGRID with a copy of the documents substantiating to be up to date regarding tax and social security obligations via the certificates issued for such purposes by the pertinent authorities.

e) AVANGRID shall not be held liable for any present or future occupational liability, and may, at any time, call on the Partner to provide documentary proof of being up to date with the latter's obligations concerning the persons assigned to the Service.

Consequently, Partner shall organise its work in the manner most suited for properly providing the services in the agreed terms and conditions, and appoint and maintain an officer as authorised representative for giving direct instructions to the personnel on its staff, and taking on work activity, organisational and managerial functions either directly or through assigned managers and coordinators required in each case for the proper execution of the service.

Partner shall provide the human resources involved in delivering these services with the necessary equipment, tools and means of production, communication and security, and group them together in a common environment that affords the required security and confidentiality.

Partner must supply all the resources required to hold tracking and control meetings: projector and video conference rooms.

AVANGRID reserves the right to request the replacement of any resource directly involved in providing the service. Partner will have a maximum term of **two (2) weeks** to make any such replacement. Partner will guarantee the replacement with a resource who meets the requirements of the Service.

HW and SW resources

Partner will provide all the HW/SW and Communications infrastructures, including elements needed by personnel (such as PCs,...), necessary for delivering the Service during the valid duration of the AGREEMENT. The cost of these resources is included in the Service price.

Security

General

The personnel of the Partner will be subject to the same security policies, criteria and procedures established by AVANGRID, both present and future, related to the requirements of the service to be provided.

Communications and Networks

- Any remote connectivity for support services will be provided through Citrix.
- FTP connections shall be encrypted and authenticated.

- This type of connection must be used for any exchange of information related to the delivery of the services described in this contract. Failing that, alternative secure channels must be established.
- As a general rule, connections between the network of any of the subcontractors of the Partner and the AVANGRID network will not be permitted. Should these prove necessary, they will only be enabled subject to authorization by AVANGRID.
- As a general rule, direct connections to the AVANGRID network by users of the Partner will not be permitted. Should these prove necessary, they will only be enabled subject to authorization by AVANGRID.
- Should the awardee company use public communication lines in its own infrastructure or for connection to the subcontractors for the delivery of this service, security conditions identical at least to those established for connection between their network and the AVANGRID network must be maintained.

Logical Access Control

- To ensure the principles of usage requirement and information confidentiality, as well as compliance with the current legislation in force, any granting of permissions for accessing the assets and resources of AVANGRID must follow the procedures established by AVANGRID for this purpose. Under no circumstances will resources or systems containing AVANGRID information exist for which the granting of access permissions is managed in a manner not accepted or established expressly by AVANGRID.
- Partner must maintain and provide AVANGRID with the updated list of the personnel involved in the various activities, modules, environments and systems.
- AVANGRID reserves the right to monitor and audit user activity in its systems and environments, as well as to suspend, if necessary, the access rights granted.
- Particularly, AVANGRID may audit those accesses which are granted on a case by case basis to the production environments.

Physical Access Control

- Partner must establish the technical and organizational measures needed to prevent the processing of its own information assets by unauthorized personnel.
- Partner must protect the equipment against malicious software.
- Before the reuse or replacement of equipment, Partner must protect, and if necessary delete, all the information contained in such equipment, and ensure that it is not possible for unauthorized personnel to retrieve and access that information.

IT Equipment

- Partner must protect the equipment against malicious software.
- Partner must establish the technical and organizational measures needed to prevent the processing of its own information assets by unauthorized personnel.
- The personnel of the Partner must, as far as possible, avoid storing confidential information from AVANGRID on laptops. Should this be necessary by reason of the service to be provided, such information must be protected by means of encryption or any other mechanism that renders it unintelligible or prevents it from being tampered with by unauthorized personnel.
- Before the reuse or replacement of equipment, the Partner must protect, and if necessary delete, all the information contained in such equipment, and ensure that it is not possible for unauthorized personnel to retrieve and access that information.

Analysis

Partner must inform AVANGRID of any incidents related to the following events:

- Unauthorized access: access or attempted access to systems, equipment, applications, files, etc. by unauthorized persons (or programs).
- Data loss: total or partial loss of information for various reasons.
- Uncontrolled distribution: sending of information to persons who should not receive it.
- IT equipment/media theft.
- Virus/malicious software attacks that may affect the exchange of information between the Partner Company and AVANGRID.
- Other: any irregularity or deficiency detected relating to violation of the criteria listed in this document.

Media

- Partner must establish adequate procedures for managing the media containing information related to the service to ensure its protection against loss or unauthorized processing.
- Paper media should be destroyed once they are no longer needed. The destruction mechanism must ensure that the information stored on the documents cannot be retrieved and that unauthorized personnel have no access to the documents.
- The media distribution mechanisms (hardcopy, magnetic, etc.) will safeguard the confidentiality and integrity of the information stored and prevent access to the media by unauthorized personnel.

Confidentiality

Partner undertakes on behalf of itself and its employees and subcontracted third parties to safeguard the strictest reserve and confidentiality regarding all data or information pertaining to AVANGRID that it may come to know during the service delivery, regardless of the cause of the access or knowledge of data or reports, and refrain from using them for any purpose other than execution of the service.

Information property

AVANGRID will remain the owner of all information. In this sense, the Partner is not entitled to the use of such information in any activity outside the execution of this service.

Partner shall provide the services by applying the usual practice of the industry in implementing and maintaining security policies and procedures to protect information of AVANGRID, which includes back-up planning, adoption of a contingency plan for disasters, not testing with real data for any test environment, ongoing assessment of the adequacy of internal controls, etc.. AVANGRID may revise these controls with the periodicity deemed appropriate.

Data protection

Should it be necessary to treat personal data files belonging to AVANGRID group companies, Partner must meet the requirements set out by the applicable Personal Data Protection laws in force. In this sense, any personal data processing shall be subject to an agreement among AVANGRID and the Partner.

Intellectual Property of the Products

Partner must accept explicitly this intellectual property clause, which establishes that the ownership of all products and processes derived from the provision of this service shall exclusively and entirely correspond to AVANGRID.

AVANGRID is the exclusive holder of the intellectual property rights for all modules, systems, component models and any works derived which may have been produced during the provision of the service and which may have been necessary for its correct execution, regardless of whether they are the property of the Partner or not.

Accordingly, the Partner is committed to provide to AVANGRID the intellectual ownership of all derived works that may be carried out on the basis of any original works during provision of the service.

AVANGRID will own all the exploitation rights that arise from the Intellectual Property Act, for the software specifically developed for AVANGRID, following its instructions, and for all modules, and documents, in any media or format. All the exploitation rights will belong to AVANGRID indefinitely and exclusively. Such rights will apply worldwide and for the maximum period of time established by law.

Subcontracting

Unless AVANGRID consents to subcontracting, all personnel assigned to do the work under this contract will belong to the Partner, which, to all effects and under its exclusive liability, assumes the legal character of employer, with all of the inherent rights and obligations that such a condition brings with it, in full compliance at all times with current labour and company legislation so that its employees may not be considered de facto, employees of AVANGRID.

Responsibility and measures

Partner will be held responsible for all the material that AVANGRID provides to perform the activities related under these service requirements.

Partner shall cover the costs for supplying service personnel with specific HW (mobile phones, PCs etc.)

Partner shall cover the costs of background checks and have them executed for all Project Managers performing services for AVANGRID.

SCHEDULE C

Terms and Conditions

TABLE OF CONTENTS

Agreement Article - Description **Page**

ARTICLE 1 – CONTRACT DOCUMENTATION AND DESCRIPTION OF SERVICES

Pursuant to that certain Master Services Procurement Agreement (the "Agreement") between Avangrid Management Company,LLC(hereinafter, "Customer"), and [redacted] (hereinafter, "Supplier" or "Contractor"), the entity (Customer and/or Company(ies)) named in the given Purchase Order, engages the Supplier, and the Supplier hereby agrees to perform the Services.

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

All work shall be invoiced in accordance with the pricing schedule approved by Customer for the Services, "Pricing Schedule," included in ***Schedule D***, attached hereto and made a part hereof (unless otherwise agreed to in writing by the Customer).

Supplier further agrees to do the following:

A. Supplier, through its experience and the normal course of business, has included full provision for local wage rates, travel and subsistence rates, allowances and conditions, if any, as well as allowances for any other measures necessary to complete the work in a satisfactory manner in accordance with this Agreement.

B. Supplier has read, understands and shall comply with ***Schedule E***, hereby referred to as "Special Conditions", attached hereto and made a part hereof.

C. Upon execution (for purposes hereof execution means when Supplier has begun to provide Services pursuant to the Purchase Order) of a Purchase Order:

1) Supplier has examined all available records pertaining to the work.

2) Supplier further states that the Contract Price and detailed schedule for completion of the work are based on Supplier's known knowledge and judgment of the conditions and hazards involved, and not upon a representation of the Customer. The Customer assumes no responsibility for any understandings or representation made by any of their representatives during or prior to execution of this Agreement unless such understandings or representations are expressly stated in this Agreement and the Agreement expressly provides that the responsibility is assumed by the Customer.

ARTICLE 2 - CONTRACT PRICE

The Contract Price for the Services (made up of the costs, fees and expenses arising under Article 3 below) shall be set forth in the Purchase Order and shall be considered fixed unless stated otherwise (time and equipment, for example) on the face of the Purchase Order.

ARTICLE 3 - REIMBURSABLE ITEMS

The Supplier shall be reimbursed for the following items for Services performed under this Agreement:

A. Fees

Supplier shall be paid at the rates per hour specified in ***Schedule D*** to the Agreement for time spent in the actual performance of Services hereunder, including the preparation of reports, UNLESS a predetermined firm lump sum price has been agreed upon by both parties for all or part of the work, the criteria of which would take precedence as referenced therein. Time spent in Normal Commuting is not a billable expense. The term "Normal Commuting" means Supplier's first trip to any Work Location in a given day and Supplier's last trip from any Work Location in a given day. The term "Work Location" shall mean any location at which Services are or are to be performed by the Supplier. The term "Supplier's Base" shall mean the location or respective locations (which shall be disclosed to Customer in advance) from which Supplier will normally travel to Work Locations to perform Services. The Supplier agrees whenever possible, to coordinate travel arrangements that will maximize time spent in performing Services for the Customer.

(i) Customer will not reimburse Supplier for additional expenses invoiced separately under a fixed bid project. The Supplier must include all the expected expenses from the quoted project within the fixed bid proposal.

(ii) Customer reserves the right to renegotiate or reject expenses when the Supplier's local office personnel are not utilized for the awarded project but meet the required job classification/criteria to complete the project and Supplier utilizes resources from other Supplier's offices.

B. Travel Expenses

Refer to Schedule B

ARTICLE 4 - PAYMENTS

A. Payments of any undisputed portions of an invoice will be made by the 60th day after the receipt by Customer of a properly completed invoice, supported by original receipts, and detailing the travel expenses.

B. An original and copy of each invoice are to be mailed to the "Bill to Location" provided in the Purchase Order.

Each invoice shall show the Purchase Order Number, Supplier work location, payment terms and the job name and other information, which may be required or reasonably requested by Customer.

The following documentation must accompany each invoice:

(i) Summary statements listing employee name, job classification, hours charged and hourly billing rates (both straight time and overtime if applicable) and total charges for the invoice period.

(ii) Copy of invoices for material, services, rentals, contracts, and other items purchased or rented in connection with the Services.

(iii) Copies of expense account summary sheets for each individual performing Services will be provided. The summary sheet will summarize lodging, meals, transportation and any other expenses. The period of time will also be shown. Supplier shall retain copies of supporting documents for such expense accounts, and these will be made available for Customer review upon written request by Customer. Supplier shall preserve all pertinent records supporting payment for Services hereunder for a period of two (2) years after final payment for the Services.

(iv) For the initial invoice submitted by Supplier for the Services under this Agreement, the bank account number of Supplier to which payments should be made by Customer and/or Company under this Agreement must be provided in writing with evidence of account ownership as provided herein. For any change in such bank account information, Supplier shall at least thirty (30) days prior to the applicable payment date provide Customer and Company with an account ownership certificate acceptable to Customer for any change to the original bank account information, in addition to the requirements set forth below.

Supplier acknowledges that invoices which do not contain the above information or are not addressed as stated in the Purchase Order may cause payment delay.

A) Method of payment

All payments by Customer and/or Company will be made by bank transfer to the following bank account owned by the Supplier: the account that Supplier indicates in writing and notifies Customer at least thirty (30) days prior to the applicable payment date pursuant to the notice requirements in this Agreement . Supplier must prove the account ownership and the identifying details of the bank account.

Any change in the bank details of the Supplier must be duly notified to Customer and/or Company, including the relevant supporting documentation. Otherwise, Customer and Company will not be obligated to make payment to the new account and payment to the former account will constitute a discharge of all obligations by Customer and Company. In any case, Customer and Company may withhold the corresponding payment, without incurring any type of liability, until the provider proves reasonable evidence of the ownership of the bank account. In the event Supplier owes money to the Customer or has defaulted under this Agreement or under any other agreements with the Customer, or Supplier has failed to pay any amount owed to the Customer whether pursuant to an agreement, a statutory or regulatory fine, the imposition of statutory or regulatory damages, or otherwise (collectively, the "Obligations"), the Customer may, at its option, setoff and/or net any or all such Obligations against any amounts owed by the Customer to the Supplier.

B) Communications

Any notifications, requests and other communications by Supplier related to the administrative management and payments under this Agreement shall be made in writing through the secure communication channel implemented for that purpose by Customer and/or Company. If such secure communication channel is not available, such notifications, requests and other such communications by Supplier must be either: (i) delivered personally; (ii) sent by fax or e-mail (with confirmation); or (iii) sent by mail (with proof of delivery) to the address listed as belonging to each party in the Agreement.

ARTICLE 5 – TAXES

The Contract Price does not include sales/use taxes. Supplier shall be responsible for payment of and assumes exclusive liability for any and all contributions or taxes imposed by or required under the laws of the State of New York or any other state or Federal law, or the Federal Social Security Act or any other act, now or hereafter in effect, upon or in respect to, wages, salaries, benefits or other compensation paid to employees engaged upon or in connection with the Services. Customer shall withhold from any payments due Supplier hereunder any amounts that it is required to withhold pursuant to any Federal or State tax laws.

ARTICLE 6 – CHANGES

No changes in the Scope of Services are authorized unless made by Customer and sustained by written Supplement. A Change is an addition, deletion, or revision in the Services or an adjustment in the Contract Price or the Schedule. Changes made by Supplier, unless authorized by an executed Supplement, shall be made at the sole risk of Supplier, there being no financial recourse against Customer. No changes in the Agreement will be made without a Supplement agreed by Customer and/or Company(ies). Unless otherwise agreed, all Supplements shall be governed by the conditions of this Agreement.

ARTICLE 7 - CLAIMS/DISPUTES

A. Any claims by Supplier relating to this Agreement, must be submitted to the Customer 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 Services.

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 41 which is to be the sole legally binding forum available to the Parties for resolution of a dispute hereunder.

ARTICLE 8 – AUDIT

Supplier shall check all materials and labor entering into the Services and shall keep full and detailed accounts as may be necessary to provide proper financial management under this Agreement. At all reasonable times, the Customer shall have access to the Supplier's offices, work and records pertinent to all charges, for inspection, audit and review. Supplier shall permit such examination and make appropriate adjustments as may be required by the results of the audit. All results of these audits must be kept confidential between the Parties and their agents. This provision shall remain in effect for two (2) years following final payment under this Agreement.

ARTICLE 9 - RIGHTS, PRIVILEGES, REMEDIES; NON WAIVER

All rights, privileges and remedies afforded each of the parties hereto by this Agreement shall be deemed cumulative and the exercise of any one or more of such rights or remedies shall not be deemed a waiver of any other right, privilege or remedy provided for herein or available at law or in equity.

ARTICLE 10 - NON WAIVER OF RIGHTS

Any failure by the Customer to enforce or require the strict performance of the terms or conditions of this Agreement shall not constitute a waiver of such terms or conditions and shall not affect or impair such terms or conditions in any way.

ARTICLE 11 - SET-OFF

In the event Supplier owes money to the Customer or has defaulted under this Agreement or under any other agreements with the Customer, or Supplier has failed to pay any amount owed to the Customer whether pursuant to an agreement, a statutory or regulatory fine, the imposition of statutory or regulatory damages, or otherwise (collectively, the "Obligations"), the Customer may, at its option, setoff and/or net any or all such Obligations against any amounts owed by the Customer to the Supplier.

ARTICLE 12 - CONFLICTING DOCUMENTS

To the extent, if any, that the specifications, drawings or other documents that may be referenced herein conflict with the provisions of this Agreement, the order of precedence set forth in Section 2.2(c) of the Agreement shall govern such conflict.

ARTICLE 13 - INDEPENDENT SUPPLIER

Supplier is and shall always remain an independent contractor in its performance of this Agreement. With the exception of staff augmentation engineering services required by Customer, where Supplier's personnel work out of Customer's offices under Customer's direction, the provisions of this Agreement shall not be construed as authorizing or reserving to Customer any right to exercise any control or direction over the operations, activities, employees or agents of Supplier in connection with this Agreement. Neither Party to this Agreement shall have any authority to employ any person as agent or employee for or on behalf of the other party to this Agreement for any purpose, and neither Party to this Agreement, nor any person performing any duties or engaging in any work at the request of such Party, shall be deemed to be an employee or agent of the other Party to this Agreement.

Customer shall carry no worker's compensation insurance, health insurance or accident insurance to cover the Supplier, or any of its agents, employees or subcontractors. Customer shall not pay any contributions to Social Security, unemployment insurance, federal or state withholding taxes, or provide any other contributions or benefits which might be expected in an employer/employee relationship. The Supplier agrees to report and pay any contributions for taxes, unemployment insurance, Social Security and any other required payments himself or herself.

ARTICLE 14 – SUBCONTRACTS

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 Customer 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 Customer's Corporate Security Group. Supplier's subcontractor may not be changed except at the request of or with the written approval of the Customer, which shall not be unreasonably withheld. The Customer shall promptly notify the Supplier in writing if, after due investigation, Customer has reasonable objection to any subcontractor on such list and does not accept it. Copies of all subcontracts shall be furnished to the applicable Customer contract management representative.

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. Contractor shall assign any subcontractor warranties applicable to the Services to Customer if Supplier becomes insolvent or files for bankruptcy.

ARTICLE 15 - THIRD PARTY BENEFITS

Except as may be specifically provided for herein, no provision of this Agreement is intended or is to be construed to be for the benefit of any third party.

ARTICLE 16 – SAFETY

Customer may at any time suspend the work or any part thereof, immediately and verbally for reasons of safety. In the event of any work stoppage, Supplier shall properly protect such work as may be liable to sustain injury from any cause.

The Customer's Safety Rules and Regulations for Suppliers are attached hereto and made a part hereof, as ***Appendix 1 to this Schedule C*** and shall apply to all work performed under this Agreement.

ARTICLE 17 – ACCIDENT, SECURITY AND LOSS PREVENTION

For the protection of workers and the public, the Supplier will take all necessary and advisable precautions for the safety of all persons and property at, on, or near the work site and will erect and maintain all necessary and advisable safeguards as required by the conditions, prudent industry practice, and progress of the work. Supplier is responsible for the security and protection of its own equipment, supplies, and tools used in connection with the Services. Supplier must use due care to protect any of the Customer's or Company(ies)'s property in its possession or under its control at any time while performing the Services, which must not be less than the care exercised by Supplier with its own property, and Supplier is responsible for any damage to such property resulting from its failure to use such care. For the avoidance of doubt, this Article shall be subject to the terms of the Data Security Rider, if applicable.

ARTICLE 18 – 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***. Supplier must maintain applicable insurance for the full term of this Agreement. An insurance certificate must be mailed to Customer prior to starting Services.

ARTICLE 19 – INDEMNIFICATION

Supplier will indemnify, defend at its expense and hold harmless, to the fullest extent permissible by law, the Customer and its Affiliates, directors, officers, employees, shareholders, managers, members, partners, agents, 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 Customer (the "Indemnitee"), from and against any and all claims, demands, suits, losses, costs, fees, damages or expenses it may suffer, or for which it may be held liable, whether including, without limitation, reasonable expenses and attorney's fees incurred in the connection therewith, by reason of:

A. any patent, trademark, or copyright infringement claim, or any design, device, process or procedure used, installed or provided by the Supplier or its agents or subcontractors under this Agreement;

B. any work-related accident or injury affecting an employee, agent or subcontractor of the Supplier, arising in connection with work performed under this Agreement;

C. any claim by an agency or instrumentality of the federal, state or any local government, or by an employee, agent or subcontractor of the Supplier alleging that:

i. the Indemnitee is required to maintain worker's compensation or unemployment or any other type of insurance upon any employee, agent or subcontractor of the Supplier;
ii. the Indemnitee is liable for tax payments or withholding with respect to any employee, agent or subcontractor of the Supplier;
iii. any employee, agent or subcontractor of the Supplier is entitled to receive employee benefits from the Indemnitee, including, without limitation, vacation, deferred compensation, medical, pension, 401(k) or any other benefit available to the Indemnitee's employees; and
iv. the Indemnitee is liable to any party, for any reason, due to the negligent performance of Services or omissions by an employee, agent or subcontractor of the Supplier;

D. bodily injury, including death, to any person or persons due to the negligent, reckless or willful actions or omissions of the Supplier or its agents or subcontractors; or

E. damage to or destruction of any property, including loss of use thereof, due to the negligent, reckless or willful actions or omissions of the Supplier, or its agents or subcontractors.

Individual employees, agents and subcontractors of the Supplier who are performing services for the Indemnitee under this Agreement shall be considered to be employees, agents or subcontractors of the Supplier for all purposes under this Agreement, notwithstanding any judicial or administrative determination that such employees, agents or subcontractors of the other party should be regarded as employees under applicable law. All actions of the employees, agents and subcontractors of the Supplier under this Agreement shall be deemed to be actions of the Supplier under these indemnities and this Agreement. In furtherance of the foregoing indemnification and not by way of limitation thereof, the Supplier hereby waives any defense 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 20 – WARRANTY

The Supplier warrants that the Services performed under this Agreement shall be performed in accordance with any Customer and applicable Company's technical documentation, standards, manuals and procedure or and other procedure specified in the RFP together with the specifications set forth in a Purchase Order or elsewhere herein, and otherwise in accordance with sound and

generally accepted industry practice by those who render these types of services with that degree of skill and care as required by customarily accepted professional practices and procedures, at the time such services are performed. If the Supplier's Services are faulty, the Supplier shall for a period of one (1) year after completion of Services, without labor charge and adders or other fee to Customer, promptly re-perform such Services to the extent necessary to correct the fault therein. This provision shall not be construed to affect or limit the liability of the Supplier to third parties, Supplier's obligation to Customer pursuant to the Indemnification clause contained herein or any other remedy which may be available to Customer under applicable law. The warranty hereunder is transferable to any assignee of Customer's rights under this Agreement, including for any remaining warranty period should an assignment occur.

ARTICLE 21 - APPROVAL/ACCEPTANCE

All work under this Agreement shall be subject to the Customer's inspection and approval before payment. Acceptance of Services hereunder by Customer does not relive Supplier from any of its obligations under this Agreement or any scope of work, and does not constitute waiver of any of the rights and remedies of Customer hereunder.

ARTICLE 22 - 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), 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 Contractor'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 best 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 work so affected and to take such compensation 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.

ARTICLE 23 - TITLE AND LIENS

Supplier represents and warrants that it has title to all equipment or material furnished hereunder free and clear of all liens and encumbrances. Complete legal and equitable title to each item of equipment or material covered by this Agreement shall pass to the Customer immediately upon delivery at 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.

Supplier shall take all action reasonably necessary to discharge, remove, or satisfy any lien filed against any property of the Customer, 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 Customer, 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 Customer, the Customer 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 - PROGRESS AND COMPLETION

It is expressly understood by the Supplier that TIME IS OF THE ESSENCE in the performance of this Agreement. The Supplier shall begin the work on the date of commencement set forth in the Agreement. The Supplier shall carry the work forward expeditiously with adequate forces and shall complete it by the time work is to be completed as stated in the Agreement.

If the Supplier is delayed at any time in the progress of the work, written notice thereof, including an explanation of the cause and the anticipated duration of the delay, shall be given promptly to the Customer by the Supplier, but in no event later than five (5) days after such delay becomes apparent. Failure to give such notice promptly and within such time limit shall be deemed sufficient reason for denial by Customer of an extension of time for performance and may be deemed a default.

Failure of Supplier's subcontractor or materials and equipment suppliers to meet schedules shall not be cause for an extension of time. Supplier acknowledges that it has sole responsibility for expediting the efforts of its subcontractors, suppliers, and others.

Without prejudice to other remedies that Customer 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 Customer 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 one per cent (1%) of the Contract Price for each full calendar week's delay.

Such Delay Damages shall never exceed fifteen per cent (15%) of the Contract Price.

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 Customer 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) Customer shall be disadvantaged by failure of Supplier to meet such obligations, (ii) it would be impracticable or extremely difficult to quantify the amount of Customer'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 Customer's rights under the Agreement or Applicable Law.

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

ARTICLE 25 - EMERGENCIES

The Supplier shall perform any work and shall furnish and install any materials and equipment necessary during an emergency affecting the safety of persons and property. In all cases, Supplier shall notify the Customer of the emergency as soon as practicable, but shall not wait for instructions before proceeding to properly protect both life and property. Any additional compensation or extension of time claimed by the Supplier on account of emergency work shall be determined by mutual agreement of the parties.

ARTICLE 26 - WORK STOPPAGE

Supplier's personnel shall not honor any union picket lines or strikes nor take part in any work slowdown or stoppage nor refuse to report for work, unless such action is protected by any state or federal labor relations law. Notwithstanding the preceding sentence, it shall be the obligation of the Supplier to supply a qualified work force. Customer may terminate this Agreement if Supplier fails to provide a qualified work force within twenty-four (24) hours of Customer's notification to Supplier that a qualified work force has not been supplied.

ARTICLE 27 - TERMINATION

Customer may for any reason, with or without cause, on written notice to Supplier terminate all or any part of the unperformed portion of this Agreement upon at least thirty (30) calendar days prior written notice to Supplier without liability to Customer except as stated in this Article. Termination of a scope of work or a Purchase Order under this Article 27 does not terminate this Agreement unless expressly stated in the notice of termination. In full discharge of any obligations to Supplier with respect to this Agreement and such termination, Customer shall pay Supplier, in accordance with the payment terms of the Agreement, only for Services satisfactorily performed prior to receipt by Supplier of notice of termination; provided, however, that such payment shall not result in a total payment to the Supplier exceeding the maximum amount payable to the Supplier pursuant to this Agreement. Termination shall not relieve Supplier of any obligation which may arise out of Services performed prior to termination. In no event shall Customer be liable to Supplier for lost profit or overhead in respect of Services not performed prior to termination, unabsorbed overhead or anticipated profits on uncompleted portions of this Agreement.

In the event Supplier is in default of any of its obligations under this Agreement, Customer shall have the right, on ten (10) days written notice to Supplier, to terminate this Agreement for such default; provided, however, that Supplier shall have the right to cure by submitting a plan acceptable to the Customer to cure the default during the ten (10) day notice period in order to avoid termination and providing that such default is, in fact, cured within thirty (30) days after Supplier first received notice of the default from Customer or some other period of time acceptable to Customer. Without limiting the provisions of this Agreement, the following events shall also constitute a default by Supplier under this Agreement:

(i) 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.

(ii) There has been a material adverse change in the financial condition of Supplier that affects the ability of Supplier to perform.

(iii) 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 Customer or Company(ies).

(iv) Supplier (i) fails or refuses to comply with any applicable laws or regulatory or permitting requirements, 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 requirements within a reasonable period of time thereafter, or (C) Company(ies) or the Customer faces any civil or criminal action or penalty as a result of such non-compliance by Supplier.

(v) Any data breach as defined in the Data Security Rider, as applicable.

In the event of such termination, the preceding paragraph of this Article shall not apply and Customer shall have all rights and remedies provided by law or equity and under this Agreement. In addition, in such event, Customer may retain from any money otherwise due for Services rendered prior to termination an amount which Customer reasonably determines is adequate to cover all damage resulting from the Supplier's default. In the event that Supplier demonstrates that a cancellation for default is erroneous, the cancellation shall, at Customer's option, be withdrawn or be deemed to have been issued as a termination for convenience pursuant to the preceding paragraph and the rights and obligations of the parties hereto shall in such event be governed accordingly. The value of Services performed not in accordance with this Agreement shall be subject to audit, assessment and approval by Customer.

ARTICLE 28 – TERM AND SURVIVAL

This Agreement shall remain in effect unless otherwise terminated as provided herein, or upon receipt by Customer of Supplier's Release and Certificate Form and Final Payment is made as set forth in Article 30 below. Notwithstanding the foregoing, Articles 4 Payments, Article 5 Taxes, Article 7 Claims/Disputes, Article 8 Audit, Article 9 Rights, Privileges, Remedies, Article 10 Non Waiver of Rights, Article 13 Independent Suppliers, Article 14 Subcontractors, Article 16 Safety, Article 17 Accident, Security and Loss Prevention, Article 18 Insurance, Article 19 Indemnification, Article 22 Force Majeure, Article 23 Title and Liens, Article 31 Assignment, Article 36 Public Release of Information, Article 37 Limitation of Liability, Article 38 Confidentiality, Article 39 Equal Employment Opportunities Compliance, Article 41 Governing Laws, Article 47 Ethics, 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 29 - REMOVAL OF EQUIPMENT

In the case of termination of this Agreement for any reason whatsoever, the Supplier, if notified to do so by the Customer, shall promptly remove any part or all of Supplier's equipment and supplies from the property of the Customer, failing which the Customer shall have the right to remove such equipment and supplies at the expense of the Supplier.

ARTICLE 30 - FINAL PAYMENT

Final payment under this Agreement shall not be made until successful completion and acceptance of the work by the Customer and when requested by Customer, Supplier's delivery of a completed Release and Certificate Form, the form of which shall be provided to Supplier at the time of the request.

ARTICLE 31 - ASSIGNMENT

Supplier shall not assign all or any of its rights or obligations under this Agreement except with the prior written consent of Customer. Any assignment made without such consent shall be void ab initio.

ARTICLE 32 - SEVERABILITY

If any provision of this Agreement is unenforceable under any applicable law or is held invalid, such holding shall not affect any other provision hereof, and this Agreement shall be construed as if such unenforceable or invalid provision had never been contained herein.

ARTICLE 33 - NON WAIVER OF RIGHTS

Any failure by the Customer to enforce or require the strict performance of the terms or conditions of this Agreement shall not constitute a waiver of such terms or conditions and shall not affect or impair such terms or conditions in any way.

ARTICLE 34 - OWNERSHIP OF PLANS

All drawings, plans, specifications, reports, designs, design data, technical and scientific data, findings, recommendations and memoranda of every description whether furnished to or prepared by Supplier under this Agreement shall (i) remain the Intellectual Property of Customer or Company (as applicable); (ii) be delivered to Customer upon completion of the work or termination or cancellation of this Agreement if requested by Customer, (iii) be deemed to have been prepared by Supplier for Customer on a work-made-for-hire basis, and (iv) shall be the property of Customer and may be used by Customer for any purpose whatsoever without any claim on the part of Supplier for additional compensation. 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 Customer without further consideration all of its right, title, and interest in such drawings, plans, specifications, reports, designs, design data, technical and scientific data, findings, recommendations and memoranda of every description, including all rights of patent, copyright, trade secret or other proprietary rights in such materials.

Except as specifically authorized by this Agreement, or as otherwise authorized in writing by Customer, information and other data developed or acquired by or furnished to the Supplier in the performance of this Agreement shall be used only in connection with the work under this Agreement.

ARTICLE 35 - KEY PERSONNEL

Personnel assigned to perform work hereunder who are designated as "Key" Personnel in this Agreement specified on ***Schedule E*** of this Agreement shall devote their working time to the work as required by the Agreement Schedule of Activities and shall not be removed, without the prior written consent of Customer, until their assignments are completed. The Customer shall have the right to reject replacements for personnel.

ARTICLE 36 - 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 Customer 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 Customer which approval may be withheld without reason or explanation to Supplier.

ARTICLE 37 - LIMITATION OF LIABILITY

To the fullest extent permitted by law, Customer 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. Any damages expressly permitted under [Article 24 re: liquidated damages and/or ***Schedule E***, as applicable are not deemed to be consequential damages under this Article 37.

ARTICLE 38 – CONFIDENTIALITY

Supplier, and its employees and agents, shall treat any information, (including any technical information, experience or data) regarding Customer or Customer's plans, programs, plants, processes, costs, equipment, operations, of Customer (or of Customer's Affiliates), which may be disclosed to, or come within the knowledge of, Supplier 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 the Services hereunder, without Customer'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 Supplier or Supplier's affiliates by third parties (other than those acting directly or indirectly for or on behalf of Customer) as a matter of legal right and without restriction on disclosure, (iii) was in Supplier's possession prior to disclosure by Customer and was not acquired by Supplier or Supplier's affiliates, its employees and agents directly or indirectly from Customer or, (iv) is required by law or by any other governmental regulatory authority to be disclosed.

Any information, which is supplied by the Supplier to Customer will be similarly restricted, including clauses (i) through (iv) in the paragraph above. Customer will not disclose such information to others or publish it in any form at any time; provided, however, that notwithstanding the foregoing, Customer may disclose any such information to its Affiliates, employees, and consultants, to any regulatory agencies or instrumentalities when such disclosure is necessary, or otherwise required by law.

Each Party agrees that they will cooperate with the other in an effort to minimize the amount of such information, which will be disclosed in any such case, and to make reasonable efforts to secure confidential treatment of such information.

In no event shall Customer'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 Customer.

All inquiries by any governmental, business, or other entity, including media, regarding any work performed or to be performed by Supplier for Customer shall be directed by Supplier to Customer for response.

ARTICLE 39 - EQUAL EMPLOYMENT OPPORTUNITY COMPLIANCE

To the extent, if any, that the provisions of the following executive order and statutes, as amended or supplemented, along with their implementing regulations, apply to the performance of the Services by Supplier, the Supplier will comply with the applicable executive order, statutes and regulations: Section 202 of Executive Order 11246 (41 CFR § § 60, et seq.); Section 402 of the Vietnam Era Veterans Readjustment Act (41 CFR § § 60-250.1, et seq.); Section 503 of the Rehabilitation Act of 1973 (41 CFR § § 741.1, et seq.); and New York Executive Law §§ (5 NYCRR § § 140.1, et seq.). These regulations may require the Supplier to develop an Affirmative Action Compliance Program and file a standard Form 100 Report (EEO-1), or other reports, as prescribed.

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 40 - 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), including any damages that may be payable under Article 27. The Company shall be entitled to approve the amount, form, premium cost, and surety Company issuing such surety bond.

ARTICLE 41 - GOVERNING LAWS

The Supplier will comply with all applicable federal, state and local laws, rules, ordinances and regulations of any governmental entity, board or agency having jurisdiction over the work or the

premises, including, without limitation, Federal, state, or local laws, rules and regulations and any applicable Executive Orders (state or Federal) in the performance of the Services. 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 42 - PERFORMANCE MONITORING

Customer will evaluate Supplier's performance by utilizing Supplier Corrective Action Reports and Supplier Performance Evaluation Reports. The Supplier must provide upon request the OSHA incident rate and Experience Modification Rate for Customer's review. The Customer's Project Manager will evaluate the Supplier's performance upon the conclusion of every project by completing the specified report. The Customer will continuously monitor the Supplier's performance. Performance by a Supplier that is less than desirable may potentially eliminate this Supplier from bidding on future projects and/or lump sum projects.

ARTICLE 43 - CONTINUOUS IMPROVEMENT

Continuous improvement is the foundation of this Agreement. Supplier warrants that it will pass on to Customer in the form of price reductions fifty (50) percent of Supplier's cost savings made possible by process improvements, reductions in material costs and the like. Supplier likewise will use its best 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 Customer. Supplier has specifically identified target cost reductions of two (2) % beyond the prices shown in ***Schedule D*** for the initial term, and agrees to work diligently with Customer personnel toward attainment of this objective. 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 44 - NO DISPUTE

Supplier represents and warrants 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 Supplier's affiliates and Customer and/or and of Customer's Affiliates.

ARTICLE 45 - SECURITY REQUIREMENTS

Supplier shall comply with Customer's Security Requirements in their performance of Services as provided herein.

Services that involve access, process, storage or transmission of non-public information, the Parties agree that the Supplier and each of its subcontractors (if any) shall comply with the data security rider attached hereto as ***Schedule H*** and made a part hereof, which includes, without limitation, the following Annexes thereto:

a) Annex 1 (the "Cyber Insurance Rider")

b) Annex 2 (the "Third Party Lite Assessment"). For purposes of clarity, Supplier and each of its subcontractors (if any) agree to complete the Third Party Lite Assessment that assesses the Supplier's security program and maturity level; provided, however, additional questions may be required by Customer based on the answered submitted by Supplier.

c) Annex 3 (the "Security Scope Framework"). For purposes of clarity, Supplier and each of its subcontractors (if any) agree to complete the security scope framework; provided, however, additional questions may be required by Customer based on the answered submitted by Supplier.

ARTICLE 46 - EMPLOYEE SOLICITATION

Supplier understands and acknowledges that Customer 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 Customer. To the maximum extent permitted under applicable laws, the Supplier agrees and covenants not to directly or indirectly solicit, hire, or recruit, or attempt to solicit, hire, or recruit–any employee who has been employed by the Customer or its Affiliates during the term of this Agreement, with whom Supplier 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 the Customer 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 the Customer through majority stock or

other ownership interest, direct or indirect. Notwithstanding the foregoing, nothing in this clause shall either (i) limit Supplier from employing any person who contacts Supplier on his or her own initiative and without any solicitation by Supplier 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 47 – 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).

ARTICLE 48 – UTILIZATION OF SMALL BUSINESS CONCERNS

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 49 – 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 50 - GRATUITIES PROHIBITED

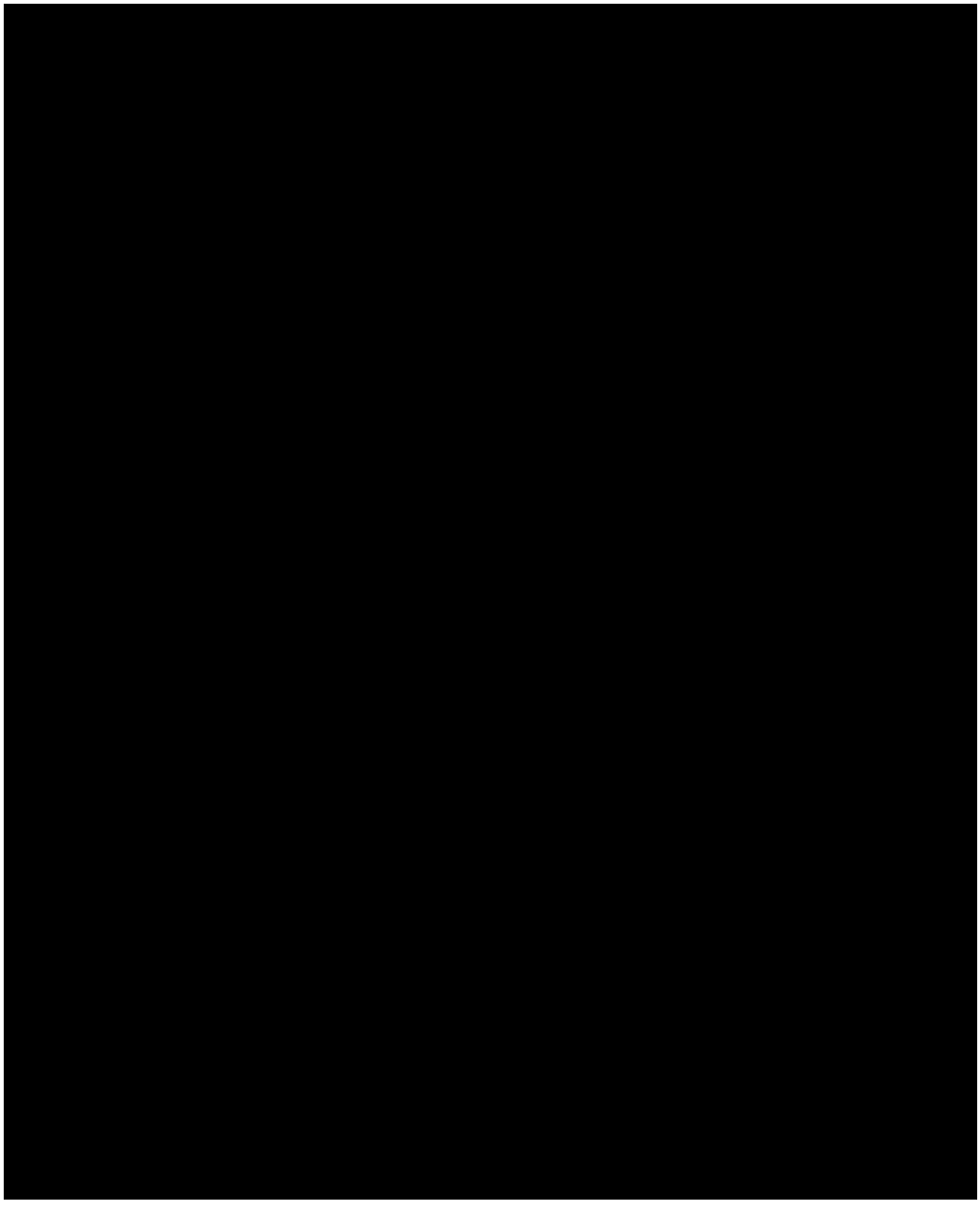
The Supplier shall not, under any circumstances, offer or extend any gratuity or special favor to any employee or agent of the Customer or its Affiliates or do anything which might reasonably be interpreted as an attempt to influence any employee or agent of the Customer in the conduct of their duties.

SCHEDULE D

Pricing Terms

1. Prices shall remain firm for orders placed during the term of this Agreement.

2. Payment Terms are Net 60 days from date of invoice.



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.

Training

Where applicable, Supplier shall provide annual on-site training, at no additional cost. Training shall be held at each Company location.

Bonding

Liquidated Damages

Retainage

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:

Unai Anton Saenz, unai.anton@avangrid.com
With Copy To : Eduardo de Frutos Salgado, eduardo.DeFrutosSalgado@avangrid.com.

Avangrid
Contract Administration
180 Marsh Hill Rd
Orange, CT 06477

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 minimums only and in no way limit the indemnification obligations of the Supplier. The actual amounts above the minimums shall be determined by 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 below.

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:

Procurement Department/ Insurance Cert.
89 East Avenue
Rochester, NY 14649-0001

A. General Insurance Requirements

Each insurance policy shall:

1) be placed with an insurance company licensed to write insurance in the State where the Services are to be performed and shall have an A.M. Best Rating of not less than "A- VII" and a policyholder surplus of at least $25,000,000.
2) have defense costs outside of the limits of liability;
3) add Customer and its Affiliates as additional insureds except of any required professional liability coverage, which shall name Customer and its Affiliates as indemnified parties;
4) not preclude Customer or its Affiliates from making claims against the policy for the wrongful acts, omissions or other tortious conduct of the Supplier/Consultant/Labor Supplier;
5) provide Customer with 30-day notice of cancellation, except for non-payment of premium and then it shall be 10 days;
6) notify Customer of any reduction in the aggregate policy limits;
7) contain a breach of warranty clause;
8) be primary and non-contributory with respect to Customer and its Affiliates;
9) contain a waiver of subrogation in favor of Customer and its Affiliates;
10) contain a separation of insureds clause;

11) contain a terrorism provision; and
12) contain a choice of law provision which states that the policy shall be governed by the State in which the Services are being performed.

B. Required Coverages

1) Workers' Compensation and Employers' Liability Insurance:

Coverage A: Statutory
Coverage B: Limits apply per issued annual policy
Bodily Injury by Accident - $500,000 each Accident
Bodily Injury by Disease - $500,000 each Employee
Bodily Injury by Disease - $500,000 Policy Limit
Policy Information Page Requirements:
Item 1 – First Named Insured and Other Named Insureds
Item 3.A. – State(s) of Operations
Item 3.C. – All Other States Except Monopolistic States
Endorsements;
Voluntary Compensation – WC 00 03 11 A
Alternate Employer – WC 00 03 01 A
FELA – If any basis
Maritime – If any basis
USL&H – If any basis

2) Automobile Liability

Combined Single Limit - $5,000,000 (limits in excess of $1M can be satisfied by umbrella/excess coverage
Uninsured/Underinsured – Minimum allowed by State law
Hired/Non-owned liability - $5,000,000

Symbol – 1

Endorsements:
Employees as Insureds
Fellow Employee Coverage
MCS 90
CA 9948

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 Amendment
Explosion, Collapse, Underground Coverage
Independent Contractors Coverage
Broad Form Property Damage
No Punitive or Exemplary Damages Exclusion
No Subsidence Exclusion

4) Umbrella/Excess Liability: Written on a Follow Form Basis and Worldwide Coverage
Per Occurrence - $5,000,000
General Aggregate - $5,000,000
Products/Completed Operations - $5,000,000
Personal & Advertising Injury - $5,000,0000

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

5) Contractor's Pollution Liability
Per Occurrence - $5,000,000
Policy Aggregate - $5,000,000

Coverage:
Environmental Impairment Liability
Bodily Injury, sickness, disease, mental anguish or shock sustained by any person, including death and mental anguish
Property Damage including physical injury or destruction of tangible property including resulting loss of use, clean-up costs, and loss of use of tangible property that has not been physically injured or destroyed
Disposal site coverage and transportation extensions
Underground storage tanks
Loss, remediation, clean-up costs and related legal expenses
Sudden and non-sudden pollution conditions
No exclusion for loss occurring over water including but not limited to a navigable waterway

Endorsements:
Extended Completed Operations – 10 years

6) Professional Liability:
Per Claim - $5,000,000

Policy Aggregate - $5,000,000
Mitigation of Loss/Rectification - $5,000,000

Coverage:

- Extended Reporting Period – 120 months
- Retroactive Date – Date of first design
- No Exclusion for environmental impairment liability
- No Exclusion for punitive damages to the extent insurable

SCHEDULE H

Data Security Rider

This Privacy and Data Security Rider (the "Rider") is entered by [redacted] ("VENDOR") and Avangrid Management Company,LLC. For the purposes of this Rider Avangrid Management 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 Services Procurement Agreement, Master Materials Agreement or other agreement between CUSTOMER and VENDOR with respect to which this Rider is being entered.

(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 Personal or Company, the parties agree that:

- The Processing activities that will be carried out by VENDOR are: access to technical documentation and technical equipment providing infrastructure services to AVANGRID IT systems. The vendor will access this data using the same methods that any other approved AVANGRID contractor following the same Acceptable Access Rule policies. Via AVANGRID document management systems (Teams, Sharepoint, share folders), via AVANGRID approved system access and via Citrix when accessing specific systems

- The categories of Personal or Company Data that will be Processed by VENDOR are: No personal Data will be accessed by the Vendor. The only company data will be that one related to technical design and IT Infrastructure architecture

  The categories of Personal Data subjects whose information will be processed by VENDOR are: No personal data will be accessed as part of this contract

- The instructions for the Processing of Personal or Company Data are: Instructions will follow AVANGRID Acceptable Access rule policies. Company data will never be moved to external data repositories or systems. Data will be flagged following company defined labelling categories, with their correspondent mechanisms to share data between AVANGRID and Vendor

(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 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 Dara 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 to carry out VENDOR's obligations under the Agreement and this Rider. Personal Data and Company Data shall only be accessed by persons who need access to carry out VENDOR's obligations under the Agreement and this Rider and in accordance with the instructions of CUSTOMER; VENDOR shall provide appropriate privacy and security training to its employees and those persons authorized to Process Personal Data or Company Data.

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

(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, VENDOR shall provide evidence that it has established and maintains Technical and Organizational Measures governing the Processing of Personal Data and Company Data appropriate to the Processing and to the nature of the Personal Data and Company Data.

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

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

(j) VENDOR shall cease Processing Personal Data and Company Data and return, 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 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 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.

***

[*Signature page follows*]

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

CUSTOMER

By: _____
Name:
Title:
Date:

By: _____
Name:
Title:
Date:

[redacted]

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

Schedule A

General Security Requirements

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

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

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

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

(b) VENDOR must, always, know the level of information protection that should be afforded to the Protected Information as well as the corresponding standards and applicable laws and regulations, and it shall adopt the Technical and Organizational Measures adequate thereto. VENDOR shall, at least, maintain Technical and Organizational Measures consistent with the type of Protected Information being processed and the services being provided by VENDOR, to secure Protected Information, which measures shall implement industry accepted protections which include physical, electronic and procedural safeguards to protect the Protected Information supplied to VENDOR against any Data Security 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 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 the Protected Information stored on it, ensuring that unauthorised personnel or third parties cannot access or recover it.

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

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

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

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

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

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

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

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

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

(j) 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 any security incident, even if it does not qualify as Data Security Breach, always within a maximum period of one (1) day after becoming aware of it, or if shorter, the shortest legal period, and shall assist and cooperate with CUSTOMER in terms of any necessary communication to third parties and other reasonable measures to remedy the situation when CUSTOMER requests it or as required by law.

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

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

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

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

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

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

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

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

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 more than one hour and always at the end of the workday.

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

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

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

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

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

iv. **Not leaving Electronic Devices in vehicles overnight,**

v. **Carrying laptops as hand luggage when traveling,**

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

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

1.6 Treatment of Information/Data

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

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

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

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

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

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

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

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

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

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

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

Avangrid Networks, Inc. – Contractor Background Check Rule

1.0 Purpose & Scope

Contractors with regular access to the premises, assets, computer systems, and\or Confidential Data of Avangrid Networks, Inc. ("Networks" or "Company") must successfully pass a background check meeting the criteria specified in this Rule. This requirement applies to all employees, agents, representatives, contractors, subcontractors, consultants, and independent contractors used by the contractor in connection with the services or work requiring such access. Unless separately defined in the body of this Rule, certain terms used in this Rule shall have the meanings ascribed in Section 6, below.

2.0 Affected Organizations

This Rule applies to Networks and all present and future subsidiaries of Networks, including but not limited to the following companies and their subsidiaries:

- Central Maine Power Company
- Avangrid Service Company
- MaineCom Services
- Maine Natural Gas Corporation
- New York State Electric & Gas Corporation
- Rochester Gas and Electric Corporation

3.0 Principles and Requirements

3.1 The safety and security of Networks' employees and property are of paramount importance. In order to safeguard these vital assets, the Company requires that those expected to have regular contact with, or access to, its employees, premises, facilities, computer systems, Confidential Data, and other key business assets not pose a potential threat to their safety, security, integrity, or well-being.

3.2 In furtherance of this objective, Networks requires that any Contractor or Contractor Representative successfully pass a Background Check as a condition both to the award of work or services under contract and to gain and maintain access to the Company's facilities, assets, Confidential Data, and\or computer systems.

3.3 Whether a Background Check is required in any given instance depends upon the type and duration of access that is required of the Contractor or Contractor Representative in order to perform the work or services. Sporadic access of short duration presenting minimal threat to Company personnel or assets may not require a Background Check, such as services provided by delivery persons, caterers, or independent contractors working remotely who do not require access to Company facilities, assets, Confidential Data, or computer systems. However, a Background Check is normally required for any Contractor or Contractor Representative who: (i) is expected to be physically present on a regular basis at a Company facility (office building or service center) without an escort (ii) is expected to require regular access to, or use of,

Confidential Data in the performance of assigned work or services, and\or (iii) is expected to require regular access to, or use of, Company computer systems, either on-site or remotely. In questionable cases not specifically addressed by this Rule, the determination whether a Background Check is required shall be made by the Director of Corporate Security.

3.4 (a) The Background Check must, at minimum, meet the criteria specified in Attachment A of this Rule and be repeated every two (2) years for Contractor(s) and Contractor Representative(s) under continuing engagements. Attachment A contains the minimum requirements for "Domestic Background Checks" and "Foreign Background Checks".

(b) A Contractor Representative who cancels, separates, or terminates his\her relationship with a Contractor must successfully pass another Background Check prior to gaining renewed access to the Company's facilities, assets, Confidential Data, or computer systems.

3.5 The terms and conditions referenced in Attachment B of this Rule must be incorporated into any contract executed with a Contractor following the effective date of this Rule. Exceptions or changes to these terms and conditions must be approved by the Legal Services Department.

3.6 The Contractor shall develop, maintain, and follow written procedures for performing Background Checks consistent with the terms of this Rule. Such procedures shall address at minimum: (i) maintenance of accurate, complete, and timely written records of completed Background Checks for the duration of the underlying contract or agreement and for six (6) years thereafter, subject to applicable legal or regulatory requirements, (ii) annual written certification that all Contractor Representatives assigned by the Contractor to provide services or work for the Company have been subjected to a Background Check compliant with this Rule and have met the requirements of the Background Check, substantially in the form of Attachment C to this Rule and (iii) an acceptable, legally-compliant process for notifying the Company of any Contractor Representative who fails to meet the minimum requirements of a Background Check.

3.7 Professional consultants and advisors, such as attorneys, auditors, and financial advisors who are not assigned to work in Networks facilities for more than two (2) weeks per year are exempt from the application of this Rule.

4.0 Rule Responsibilities and Management.

4.1 Procurement is responsible for:

4.1.1 insuring that awards and contracts with Contractors that are negotiated and processed by Procurement contain the provisions of Attachment B when requested by the Managing Department. If Procurement receives a request from the Managing Department which does not indicate the need for a Rider (Attachment B), Procurement will request that the Managing Department work with Corporate Security to determine if a Rider (Attachment B) is required.

4.2 Human Resources is responsible for:

4.2.1 verifying completion of Background Checks for all contingent worker staff, including those contingent workers who were employees of any Avangrid Networks, Inc. affiliate, prior to assignment to an Networks facility; and

4.2.2 verifying completion of Background Checks every two (2) years for temporary worker staff on extended engagement; and

4.2.3 periodically auditing the background check processes used by any Contractor supplying temporary worker staff to confirm compliance with the terms of this Rule and the applicable provisions of the Contractor's agreement; and

4.2.4 addressing the Contractor's violation of this Rule or agreement after consultation with legal counsel.

4.3 The Managing Department is responsible for:

4.3.1 advising Procurement when background checks are required under agreements or awards processed by Procurement;

4.3.2 verifying completion of Background Checks and maintaining an up to date list for all new or replacement Contractor Representatives during the course of an engagement (other than those assigned to Human Resources, above) under the management or supervision of the Managing Department; and

4.3.3 requesting from Corporate Security exceptions or waivers from this Rule in cases when a Contractor, necessary for the conduct of Company business, cannot comply with the Background Check requirements set forth herein, and

4.3.4 verifying completion of Background Checks every two (2) years for Contractor Representatives retained or supervised by the Managing Department on extended engagement; and

4.3.5 communicating the requirements of this Rule to all Networks employees and staff assigned to manage or supervise a Contractor or Contractor Representative subject to the requirements of this Rule; and

4.3.6 certifying to the Compliance Officer that Contractor Representatives assigned by the Contractor to provide services or work for the Company under the direction or supervision of the Managing Department have been

subjected to a Background Check compliant with this Rule and have met the requirements of the Background Check.

4.4 The Corporate Security function is responsible for granting waivers referenced in Attachment A and maintaining an active list of waivers that have been issued along with the documentation to support those waivers.

4.5 The Legal Services Department is responsible for approving any material modifications to the terms and conditions referenced in Attachment B of this Rule.

4.6 The Compliance Officer is responsible for communicating to Managing Departments the annual certification requirement set forth in Section 4.3.6, above.

4.7 The Audit Department is responsible for periodically auditing compliance with this Rule.

5.0 Rule Exceptions.

Any exception to this Rule, other than those exceptions specifically addressed in the body of this Rule, must be approved by the Director of Security. Any request for exception must be made in writing accompanied by supporting business documentation justifying the exception on cost\benefit, legal, regulatory, and\or other reasonable grounds.

6.0 Definitions.

Background Check: A background check conforming to the requirements of this Rule, including but not limited to the minimum criteria specified in Attachment A.

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

Contractor: Any person or entity hired or retained by Networks or its subsidiaries to perform work or services for the Company.

Contractor Representative: Any and all employees, agents, representatives, contractors, subcontractors, consultants, and independent contractors used by a Contractor in connection with the services or work requiring access to Company premises, assets, computer systems, and\or Confidential Data.

Managing Department: The Networks department, organization, or function requiring the work or services of a Contractor or Contractor Representative in connection with assigned duties or responsibilities; the Managing Department for all temporary worker staff shall be deemed to be the Human Resources Department.

Sensitive Data: That subset of Confidential Data, including Social Security number, passport number, driver's license number, or similar identifier, or credit or debit card number, whose unauthorized disclosure or use could reasonably entail enhanced potential risk for the data subject.

Attachment A – Domestic Background Checks

Background Check Criteria

1. Minimum Requirements: A background search shall consist of the following minimum elements for anyone with an SSN, which includes resident aliens:

a. Social Security Number Verification
b. Motor Vehicle Report (if driving Networks company vehicle)
c. Prohibited Parties Database Search\Debarment Lists
d. Criminal History Search
e. National Sex Offender Registry

Note: The background check on a resident alien should go back as long as they lived in the US if less than seven years. For the remainder of the 7 years, the Foreign Background Checks criteria would apply.

2. Disqualifying Offenses: The convictions shall generally require disqualification of a Contractor or Contractor Representative, based upon the nature of the work or services and the access required to perform such work or services and consistent with, and to the extent permitted by, applicable state law. This is not intended to be an exhaustive list and convictions for other crimes may also be grounds for disqualification:

a. Felonies: All felony convictions within the last seven (7) years, except as restricted by applicable federal, state and local laws.

b. Misdemeanors: The following misdemeanor convictions within a period of five (5) years, except as restricted by applicable federal, state, and local laws:

Arson	**Assault**	**Battery**
Child Abuse and Neglect	**Criminal Contempt**	**Criminal Conversion (Theft)**
Criminal Mischief	**Escape**	**Evading Arrest**
Failure to Stop	**Harassment**	**Hit and Run**
Indecent Exposure	**Injury to Personal Property**	**Larceny**
Petty Theft Possession of Controlled Drugs	**Possession of drug paraphernalia**	**Possession of marijuana**
Possession of Stolen Goods	**Prostitution**	**Purchasing Alcoholic Beverages for a Child**
Resisting Arrest	**Sexual Offenses**	**Theft by Check**
Trespassing	**Unlawful Sales to Minors (Alcohol and Tobacco)**	**Vandalism**
Violation of Probation	**Violation of Protective Order**	**Welfare Violation**

3. Time Restrictions Calculation: All hiring time restrictions for felony convictions are calculated from the date of release from incarceration.

4. Pending Charges: An individual charged with a disqualifying offense may not be hired, retained, or placed with Networks while any known charge(s) is\are pending. The individual may be considered for placement if exonerated of the charge(s).

5. Outstanding Warrants: An individual with an outstanding warrant for a disqualifying offense may not be hired, retained, or placed with Networks until the warrant has been dismissed.

6. Failure to Disclose: Any individual or Contractor who fails to disclose any felony and/or misdemeanor conviction(s) prior to the Contractor's submission of such individual's or Contractor's criminal background information may not be hired, retained, or placed with Networks.

7. Non-Disqualifying Offenses: A conviction of one of the following offenses within a five (5) year period (as long as the offenses did not occur within the previous twelve (12) months, and there are no other convictions for any other disqualifying offense:

- Breach of Peace
- Disorderly Conduct
- Failure to Appear

8. Motor Vehicle Report (MVR): The following MVR check is required prior to hiring, retaining, or placing any Contractor or Contractor Representative in a position that requires the operation of a motor vehicle on behalf of Networks:

I. Disqualifying Criteria:
   a. Invalid, suspended, or revoked drivers license;
   b. One (1) conviction of driving under the influence (DUI) within the preceding year; two (2) or more DUI convictions, no time limit;
   c. Three (3) or more moving violations within the preceding three (3) years;
   d. Any accumulation of suspensions of over one (1) year in length within the preceding three (3) years;
   e. More than two (2) accidents with indication of fault within the preceding three (3) years.

9. Debarment Lists: All Contractors and Contractor Representatives shall be checked against the debarment\exclusion lists maintained by the following agencies:

- Federal Department of Health and Human Services;
- General Services Administration
- Federal Food and Drug Administration.

Attachment A – Foreign Background Checks

Background Check Criteria

1. Minimum Requirements: A background search shall consist of the following minimum elements for non US Citizens:

NERC CIP Access. When Networks 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.

- For someone who has resided and/or worked outside of Spain in the last 7 years, the vendor should perform an International Background Check to show the absence or existence of a criminal record. International background checks should verify known data such as employment, education, criminal and civil records, travel and immigration records, as well as address and identity verification

- For someone who has resided and worked only in Spain for the last 7 years, their passport and recent Criminal Record Certificate from the Spanish Ministry of Justice is sufficient (assuming it shows the absence of a criminal record).

- Due to EU privacy rules, the Criminal Record Certificate can only be supplied to the applicant after proof of identify. The Certificate certifies the absence or existence of a criminal record. If the applicant is not willing to obtain and provide the Certificate, an International Background Check should be conducted.

Non CIP Access. When Networks determines that the Contractor engagement is such that compliance with NERC CIP Standards is not required, the background check needs to include the following:

- For someone who has resided and/or worked outside of Spain in the last 7 years, the vendor should include identity verification and perform an **International Background Check** to show the absence or existence of a criminal record. The international background check should verify known data such as employment, education, criminal and civil records, travel and immigration records, as well as identity.

- For someone who has resided and worked only in Spain for the last 7 years, a **certificate duly signed** by the vendor is sufficient if it states that its employee(s) assigned to work for Avangrid Networks, Inc. (i) are duly affiliated to the Spanish Social Security and (ii) have the necessary academic and professional experience.

2. Disqualifying Offenses: Any past convictions for a crime shall generally require disqualification of a Contractor or Contractor Representative, based upon the nature of the work or services and the access required to perform such work or services and consistent with, and to the extent permitted by, applicable law.

Attachment B – Domestic Background Checks

Contract Language

Direction: The following provision must be added to all contracts with Contractors subject to this Background Check Policy:

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 Avangrid Networks, Inc. –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 Attachment A of 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.

Attachment B – Foreign Background Checks

Contract Language

Direction: The following provision must be added to all contracts with Contractors subject to this Background Check Policy:

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 Avangrid Networks, Inc. –Contractor Background Check Rule, as such Rule may be revised and\or supplemented from time to time, which Rule 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:

NERC CIP Access. If applicable (i.e., when Networks 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.

- For someone who has resided and/or worked outside of Spain in the last 7 years, the contractor should perform an International Background Check to show the absence or existence of a criminal record. International background checks should verify known data such as employment, education, criminal and civil records, travel and immigration records, as well as address and identity verification

- For someone who has resided and worked only in Spain for the last 7 years, their passport and recent Criminal Record Certificate from the Spanish Ministry of Justice is sufficient (assuming it shows the absence of a criminal record).

- Due to EU privacy rules, the Criminal Record Certificate can only be supplied to the applicant after proof of identify. The Certificate certifies the absence or existence of a criminal record. If the applicant is not willing to obtain and provide the Certificate, an International Background Check should be conducted.

Non CIP Access. To comply, the background check needs to include the following:

- For someone who has resided and/or worked outside of Spain in the last 7 years, the vendor should include identity verification and perform an **International Background Check** to show the absence or existence of a criminal record. The international background check should verify known data such as employment, education, criminal and civil records, travel and immigration records, as well as identity.

- For someone who has resided and worked only in Spain for the last 7 years, a **certificate duly signed** by the vendor is sufficient if it states that its employee(s) assigned to work for Avangrid

Networks, Inc. (i) are duly affiliated to the Spanish Social Security and (ii) have the necessary academic and professional experience.

The Background Check must be completed prior to initial access by Contractor Representative(s) and must, at minimum, meet the criteria specified in Attachment A of 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.

Avangrid Networks, Inc. – Contractor Background Check Rule

Attachment C

Contractor Certification Form

The undersigned agent of _____ **certifies** that the employees, contractors, or subcontractors listed below meet the requirements agreed to in Attachment B of the Rule.

It is the responsibility of the vendor to notify Avangrid Networks, Inc. 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 Avangrid Networks, Inc. are in good standing and have been in good standing since their last background check.

_____ _____
Signature Date

_____
Printed Name and Position