ORD 25-064

AN ORDINANCE TO AUTHORIZE AND APPROVE A NETWORK-AS-A SERVICE AGREEMENT BETWEEN THE CITY OF WILMINGTON AND DELMARVA POWER & LIGHT COMPANY

#0132

Sponsor:

Council Member Oliver

WHEREAS, pursuant to Section 2-308 and Section 8-200 of the City Charter, the City of Wilmington is authorized to enter into contracts for the supply of personal property or the rendering of services for a period of more than one year if approved by City Council by ordinance; and

WHEREAS, the City would like to enter into a Network-As-A-Service Agreement with Delmarva Power & Light Company ("Delmarva") for the City and Itron, Inc. to use Delmarva's Automated Metering Infrastructure Mesh Network to collect water meter usage information from City water meters (the "Agreement"), a copy of which, in substantial form, is attached hereto and incorporated by reference herein as Exhibit "A"; and

WHEREAS, the term of the Agreement is for a period of five (5) years with two (2) five-year extension options at an estimated price of Ninety-One Thousand Two Hundred Dollars ($91,200.00) for the first year with an approximately three percent (3%) increase for each year thereafter; and

WHEREAS, it is the recommendation of the Department of Public Works that City Council authorize the City to enter into the Agreement with Delmarva for a period of five (5) years with two five-year extension options thereafter; and

WHEREAS, City Council deems it necessary and appropriate to authorize the City to enter into the Agreement with Delmarva for a period of five (5) years with two five-year extension options thereafter.

NOW, THEREFORE, THE COUNCIL OF THE CITY OF WILMINGTON HEREBY ORDAINS:

SECTION 1. The Agreement (being a Network-As-A-Service Agreement between the City of Wilmington and Delmarva Power & Light Company), a copy of which, in substantial form, is attached hereto as Exhibit "A," for the period of five (5) years with two (2) five-year extension options thereafter, at an estimated price of Ninety-One Thousand Two Hundred Dollars ($91,200.00) for the first year with an approximately three percent (3%) increase for each year thereafter, is hereby approved, and the Mayor, or his designee, is hereby authorized to execute as many copies of the Agreement, as well as to take all additional undertakings related thereto, as may be necessary.

SECTION 2. This Ordinance shall become effective upon its passage by City Council and approval by the Mayor.

First Reading..... November 6, 2025
Second Reading..... November 6, 2025
Third Reading.....

Passed by City Council,

_____
President of City Council

ATTEST:_____
City Clerk

Approved this ____ day of _____, 2026.

_____
Mayor

SYNOPSIS: This Ordinance authorizes the City to enter into a five-year Network-As-A Service Agreement (the "Agreement") with Delmarva Power & Light Company for the City and Itron, Inc. to use Delmarva's Automated Metering Infrastructure Mesh Network to collect water meter usage information from City water meters. The Agreement contains two (2) five-year extension options.

FISCAL IMPACT STATEMENT: The Office of Management and Budget has reviewed and analyzed this Ordinance and the Agreement attached as Exhibit A. The Agreement supports operational efficiencies in water meter data collection but represents a recurring operating expense commitment over a multi-year period. The estimated cost for the first year of the Agreement is $91,200, with an approximate annual increase of three percent (3%) thereafter. Based on the stated escalation, the projected total cost over the initial five-year term is approximately $484,000. Should both five-year renewal options be exercised, total expenditure over the full potential fifteen-year term is estimated to exceed $1.5 million, subject to annual price adjustments and actual service levels. Funding for the Agreement is supported through the Water/Sewer Fund operating budget, which is subject to annual appropriation by City Council. Ongoing costs will need to be incorporated into future operating budgets for the duration of the contract term.

W0130369

EXHIBIT A

NETWORK-AS-A-SERVICE AGREEMENT

This Network-as-a-Service Agreement, dated as of the Effective Date (defined below), between Delmarva Power & Light Company, a Delaware and Virginia corporation **("DPL")**, and City of Wilmington, a Delaware municipal corporation **("Customer")**. Each of DPL and Customer are a **"Party"** and together are the **"Parties"**.

The Parties now wish to enter into an agreement under which DPL will expand the use of its AMI Mesh Network to collect water usage information from Customer's water meters in a production environment as described in this Agreement's Schedule A Description of Services. The Parties, therefore, with the intent to be legally bound, agree as follows:

1. DEFINITIONS

In addition to the terms defined elsewhere in this Agreement, the following terms shall have the respective meanings specified below:

"Action" means any claim, action, cause of action, demand, lawsuit, arbitration, audit, notice of violation, proceeding, litigation, citation, summons, or investigation of any nature, civil, criminal, administrative, regulatory, or other, whether at law, in equity, or otherwise.

"Affiliate" means, with respect to a Person, any entity which directly or indirectly, through one or more intermediaries, is Controlled by or is under Common Control with such Person.

"Agreement" means this Network-as-a-Service Agreement, together with all schedules, exhibits, attachments, addenda, and any other documents made under and specifically referencing this Network-as-a-Service Agreement.

"AMI Mesh Network" means a group of devices that connect wirelessly to act as a single wireless network that is used to allow two-way communication between a smart utility meter and the utility company or other Person including its Headend System.

"Availability Percentage" has the meaning given in Schedule B.

"Available" has the meaning given in Schedule B.

"Commercially Reasonable Efforts" means taking such steps and performing in such a manner as a company would undertake where it was acting in an objectively prudent and reasonable manner, by reference to established customs and practices, where such customs and practices exist, to achieve a particular desired result for its own benefit or to discharge an obligation to another party.

"Confidential Information" means information in any form or medium (whether oral, written, electronic, or other) that the Disclosing Party considers confidential or proprietary, including information consisting of or relating to the Disclosing Party's technology, trade secrets, know how, business operations, plans, strategies, customers, customer usage data, and pricing, and information with respect to which the Disclosing Party has contractual or other confidentiality obligations, in each case whether or not marked, designated, or otherwise identified as "confidential."

"Control" means possessing, directly or indirectly, the power to direct or cause the direction of the management, policies or operations of an entity, whether through ownership of voting securities, by contract or otherwise, and "Controlled" and "Common Control" have correlative meanings.

"Customer" has the meaning given to it in the preamble to this Agreement.

"Meter Data" means data provided by or on behalf of Customer to DPL via DPL's AMI Mesh Network under this Agreement.

"Disclosing Party" has the meaning given to it in Section 8.1.

"Effective Date" means the latest date on which this Agreement is executed by a Party.

"Feedback" has the meaning given to it in Section 7.2.

"Force Majeure Event" has the meaning given to it in Section 12.1.

"Governmental Authority" means applicable United States territory, state and federal governments, agencies, including interagency bodies, and any court or regulatory, administrative, judicial, executive, legislative or governmental entity thereof.

"Headend System" means software designed to help utility operators collect and manage advanced metering infrastructure meter consumption data.

"Impacted Party" has the meaning given to it in Section 12.1.

"Initial Term" has the meaning given to it in Section 5.1.

"Instance of Unavailability" has the meaning given to it in Schedule B.

"Law" means, collectively, (i) all laws, statutes, regulations, rules and ordinances of any Governmental Authority, (ii) written regulatory guidance, written substantive recommendations or directives, written opinions and written interpretations, policies and guidelines of any Governmental Authority, and (iii) rulings, injunctions, judgments and orders issued by any Governmental Authority, each of (i) through (iii) as amended and replaced from time to time.

"Losses" means losses, adverse claims, penalties, fines, judgments, damages, liabilities and expenses (including reasonable attorneys' fees, expert witness fees, expenses and costs of settlement).

"Measurement Period" means a calendar month.

"Milestone" has the meaning given to it in Schedule A.

"Network" means DPL's AMI Mesh Network, its backhaul network, and other parts of

DPL's network connecting its Network Devices to its Headend System.

"Network Device" means a device on DPL's AMI Mesh Network to which a Provisioned Water Meter connects.

"Party" has the meaning given to it in the Preamble to this Agreement.

"Person" means an individual, corporation, partnership, limited partnership, limited liability partnership, limited liability company, joint venture, association, trust, unincorporated organization, Governmental Authority or other entity.

"Provisioned Water Meter" means a Water Meter that has successfully connected to and transmitted data to a Network Device.

"Receiving Party" has the meaning given to it in Section 8.1.

"Renewal Term" has the meaning given to it in Section 5.2.

"Resultant Data" means anonymous or anonymized data and information that is collected or generated by DPL that is related to or generated from Customer's use of the Services.

"Services" means the services provided under this Agreement as described in Schedule A

including the Steady-State Services.

"Steady-State Services" has the meaning given to it in Schedule A.

"Term" has the meaning given to it in Section 5.2.

"Water Meter" means Customer water meters.

2. SERVICES

2.1. Provision of Services. DPL shall provide the Services to Customer as described in Schedule A and in accordance with the terms and conditions of this Agreement and conditioned on the successful completion, as determined by DPL, of Exelon's ("**Exelon**") and DPL's architectural review process or their solutions design review approval process.

2.2. Changes to Network or Services. DPL may at any time change the AMI Mesh Network or the Services if it is required to do so to comply with applicable Law or where it is required in DPL's business judgment for operational reasons so long as such changes do not diminish or disrupt DPL's ability to provide the Services to Customer.

2.3. Suspension of Services. DPL may, directly or indirectly, suspend or otherwise deny one or more Water Meter's access to or use of all or any part of the AMI Mesh Network, without incurring any resulting obligation or liability, if: (i) DPL receives a judicial or other governmental demand or order, subpoena, or law enforcement request that expressly or by reasonable implication requires DPL to do so; or (ii) DPL believes, in its reasonable discretion, that: (a) Customer, after notice, has failed to comply with Section 2.4 as it relates to the relevant Water Meters; (b) such suspension or denial is, in DPL's reasonable discretion, necessary to prevent damage, disruption, or other harm to the AMI Mesh Network, the DPL Headend System, a Network Device, or any other DPL property. This Section 2.3 does not limit any of DPL's other rights or remedies, whether at law, in equity, or under this Agreement. If DPL exercises its authority under this Section 2.3, it shall deliver notice of such action to the Customer as soon as practicable. If DPL suspends Services pursuant to this Section 2.3, the Fees (defined below) shall be correspondingly prorated.

2.4. Use Restrictions. Customer may not use the Services to: (i) transmit or otherwise distribute information constituting or encouraging conduct that would constitute a criminal offense or give rise to civil liability or otherwise use the Services in a manner contrary to Law or in a manner that would restrict or inhibit any other user from using the Services; (ii) transmit any information that contains a virus, Trojan horse, or other harmful or disruptive component; (iii) transmit or otherwise distribute information that is protected by copyright or other intellectual property rights without prior authorization from the rights holders or that constitutes an invasion of privacy; (iv) cause or create risk of causing an invasion of privacy in violation of applicable Law or (v) violate any system or network

security measures including engaging in unauthorized access to DPL's or a third party's network, data, or information.

2.5. Monitoring of Data. DPL has no obligation but has the right at any time and from time to time, as part of the management of its AMI Mesh Network and the Services, to monitor the Meter Data transmitted using the Services. DPL shall have no responsibility for inaccurate or incomplete Meter Data except to the extent such inaccuracy or incompleteness results from DPL' s breach of this Agreement.

2.6. Project Managers. Each Party shall designate an individual as a project manager who is the primary point of contact for the other Party for matters related to the Services and shall designate an individual as an alternate in the event that the designated project manager is not available. The Parties shall agree upon a schedule for the project managers to meet and confer regarding the Services and may agree to add or remove additional project managers to focus on particular aspects of the Services as necessary.

2.7. Effect of DPL Failure or Delay. If Customer's performance of its obligations under this Agreement is prevented or delayed by any act or omission of DPL or its agents, subcontractors, consultants, or employees, Customer shall not be deemed in breach of its obligations under this Agreement or otherwise liable for any Losses incurred by DPL, in each case, to the extent arising directly or indirectly from such prevention or delay.

2.8. Access and Security. DPL shall use Commercially Reasonable Efforts designed to protect against any unauthorized access to or use of the Network and shall notify Customer promptly of any such unauthorized access or use where DPL believes that such access or use resulted in actual or suspected access to Meter Data.

3. CUSTOMER OBLIGATIONS

3.1. Customer Cooperation. Customer shall cooperate with DPL and provide reasonable assistance to enable DPL to carry out its obligations under this Agreement, respond within ten (10) business days to any DPL request to provide direction, information, approvals, authorizations, or decisions that are reasonably necessary for DPL to perform Services in accordance with the requirements of this Agreement.

3.2. Customer Equipment. Customer shall, at its own cost, prepare and install its Water Meters in accordance with DPL's written requirements and instructions prior to the commencement of Services for such Water Meters. Customer shall be solely responsible to ensure that all Water Meters (i) are in good working order and suitable for the purposes for which they are used in relation to the Services and (ii) conform to all relevant legal or industry standards or requirements.

3.3. Third-Party Approvals. Prior to the start of the Services and throughout the Term, Customer shall obtain and maintain all necessary licenses and consents and comply with all relevant Laws applicable to its provision of Meter Data to DPL and DPL's provision of data to (including DPL's use of as applicable) Customer's Headend System and as otherwise reasonably necessary for Customer to meet its obligations under this Agreement, and provide proof of same upon DPL's request.

3.4. Effect of Customer Failure or Delay. If DPL's performance of its obligations under this Agreement is prevented or delayed by any act or omission of Customer or its agents, subcontractors, consultants,

or employees, DPL shall not be deemed in breach of its obligations under this Agreement or otherwise liable for any Losses incurred by Customer, in each case, to the extent arising directly or indirectly from such prevention or delay.

3.5. Access and Security.

3.5.1 Customer shall comply with all rules, regulations, and policies of DPL that are made available to Customer in writing regarding the Network, the Network Devices, and Water Meters' and Meter Data's access and connection thereto, including compliance with the attached Schedule D – Exelon's Exhibit H – Basic Cyber and Information Security Special Terms and Conditions, incorporated by reference herein. Customer shall use Commercially Reasonable Efforts to prevent unauthorized access to or use of the Services and Network and notify DPL promptly of any such unauthorized access or use.

3.5.2 Customer shall not access any Provisioned Water Meter with any field service tools other than those that are approved by Itron in advance.

3.5.3 At least every three (3) years, DPL may perform cybersecurity assessments and penetration testing of the DPL Network and the Provisioned Water Meters at DPL's sole cost and expense, and Customer shall provide reasonable cooperation and support of such assessments and penetration testing. To the extent any issues identified during such assessments and penetration testing relate to the Provisioned Water Meters or Customer's cooperation is otherwise necessary to resolve such issue, Customer shall reasonably cooperate with DPL in resolving such issues.

4. CHANGE ORDERS

4.1. Change Request. If either Party wishes to change the scope or performance of the Services, it shall submit details of the requested change to the other Party in writing. DPL shall, within a reasonable time after receiving a Customer-initiated request, state if DPL is willing to consider Customer's request, or at the same time that DPL initiates such a request, provide a written estimate to Customer of: (i) the estimated time necessary to implement the change; (ii) any changes to the Fees and other charges for the Services that would arise from the change; (iii) the anticipated effect of the change on the Services; (iv) any other information reasonably requested by Customer to allow Customer to evaluate the proposed change.

4.2. Agreeing on a Change Order. Promptly after receipt of the written estimate, the Parties may negotiate and agree in writing on the terms of such change (a **"Change Order"**). Neither Party shall be bound by any Change Order unless agreed upon in writing in accordance with Section 13.9.

5. TERM AND TERMINATION

5.1. Initial Term. The initial term of this Agreement commences as of the Effective Date and, unless terminated earlier pursuant any of the Agreement's express provisions, will continue in effect for five (5) years (the **"Initial Term"**).

5.2. Renewal Terms. Customer shall have the option to extend the Initial Term of this Agreement for two (2) successive five (5) year periods (each a **"Renewal Term"** and, collectively, together with the Initial Term, and the Transition Period, the **"Term"**). Customer shall provide notice of its intent to exercise the option for each Renewal Term at least one hundred eighty (180) days in advance of the

commencement of each Renewal Term. DPL may accept notice of less than one hundred eighty (180) days if it chooses.

5.3. Transition Period. Following the end of the Term, whether at the end of an Initial Term, a Renewal Term, or if the Agreement has been terminated early under Section 5.4, the Agreement shall continue for a transitional period of six (6) months (the **"Transition Period"**). During the Transition Period, DPL and Customer will work together to develop and implement a plan to support Customer transitioning from the Services (such plan when approved in writing by each of the Parties, the **"Transition Plan"**). During the Transition Period, no new Water Meters may be added to the Network as Provisioned Water Meters, but the Services will continue for the Provisioned Water Meters that were connected to the Network prior to the start of the Transition Period and that have not yet been disconnected from the Network including pursuant to the Transition Plan. In addition to the Fees provided for in Section 6, if the Agreement is terminated by reason of a default or non-renewal by Customer, Customer shall reimburse DPL for DPL's reasonable, out of pocket costs in developing and implementing the Transition Plan in advance. If DPL provides notice of non-renewal under Section 5.2, DPL must provide to Customer at the same time as such notice an initial technology and system roadmap to serve as the basis for negotiating a Transition Plan.

5.4. Mutual Termination Rights. In addition to any other express termination right set forth elsewhere in this Agreement: (i) either Party may terminate this Agreement, effective on written notice to the other Party, if the other Party materially breaches this Agreement, and such breach: (a) is incapable of cure; or (b) being capable of cure, remains uncured sixty (60) days after the non-breaching Party provides the breaching Party with written notice of such breach; and (ii) either Party may terminate this Agreement, effective immediately upon written notice to the other Party, if the other Party: (a) becomes insolvent or is generally unable to pay, or fails to pay, its debts as they become due; (b) files, or has filed against it, a petition for voluntary or involuntary bankruptcy or otherwise becomes subject, voluntarily or involuntarily, to any proceeding under any domestic or foreign bankruptcy or insolvency Law; (c) makes or seeks to make a general assignment for the benefit of its creditors; or (d) applies for or has appointed a receiver, trustee, custodian, or similar agent appointed by order of any court of competent jurisdiction to take charge of or sell any material portion of its property or business.

5.5. Termination Based on Technical Changes.

If Customer migrates its Water Meters or Headend System to Water Meters or Headend System that is not capable of communicating with DPL's Network in a manner that makes provision of the Services commercially unreasonable for either Party to continue, the Parties may agree to terminate the Agreement and Customer shall be responsible for all reasonable costs of executing the Transition Plan. Additionally, Customer shall be responsible for the cost of stranded assets deployed by DPL in order to provide the Services in an amount equal to twenty-five percent (25%) of the Fees remaining in the then current five (5) year portion of the Term after the effective date of termination of the Agreement.

If DPL modifies its Network or Headend System to a Network or Headend System that makes provision of the Services commercially unreasonable for either Party to continue, the Parties may agree to terminate the Agreement. The Parties will negotiate in good faith to agree upon terms under which: (i) Water Meters or Headend System can be modified in order to make the provision of Services commercially reasonable to continue; or (ii) DPL would sell existing Network hardware to Customer

for Customer to own and operate its own private mesh network based on book value with a fifteen (15) year depreciation schedule. If there is a Transition Plan as a result of DPL modifying its Network Headend System, DPL shall be solely responsible for the costs for implementation of the Transition Plan.

5.6. Effect of Termination or Expiration. Upon any expiration or termination of this Agreement, except as expressly otherwise provided in this Agreement: All rights, licenses, consents, and authorizations granted by either Party to the other hereunder will immediately terminate.

DPL shall cease all use of any Meter Data and Customer Confidential Information and (i) promptly return to Customer, or at Customer's written request destroy, all documents and tangible materials containing, reflecting, incorporating, or based on Meter Data or Customer's Confidential Information; and (ii) permanently erase all Meter Data and Customer Confidential Information from all systems DPL directly or indirectly controls, provided that, for clarity, DPL's obligations under this Section 5.6.2 do not apply to any Resultant Data.

Customer shall immediately cease all use of any Services and, except to the extent prohibited by the Delaware Freedom of Information Act ("**FOIA**"): (i) promptly return to DPL, or at DPL's written request destroy, all documents and tangible materials containing, reflecting, incorporating, or based on DPL's Confidential Information; (ii) permanently erase DPL Confidential Information from all systems Customer directly or indirectly controls; and (iii) render all Water Meters and associated interface management units unable to connect to the DPL Network including by installing or having installed firmware that is incapable of connecting such Water Meters to the DPL Network.

Customer shall return to DPL any equipment and software provided by or on behalf of DPL to enable Customer to access or test the Services including field service units, access points, and electric meters.

5.7. Surviving Terms. The provisions set forth in the following sections, and any other right or obligation of the Parties in this Agreement that, by its nature, should survive termination or expiration of this Agreement, will survive any expiration or termination of this Agreement: Section 2.4, Section 5.6, Section 5.7, Section 8, Section 9.2, Section 10, Section 11, and Section 13.

6. FEES AND EXPENSES; PAYMENT TERMS

6.1. Fees. Customer shall pay to DPL the fees described in Schedule C ("**Fees**").

6.2. Taxes. All charges and Fees to be paid by Customer under the Agreement are exclusive of any applicable withholding, sales, use, excise, value added or other taxes and municipal fees, excluding any taxes on DPL's property, income or payroll. Any such taxes or fees for which DPL is responsible to collect from Customer shall be billed by DPL and paid by Customer. Customer shall reimburse DPL for any penalties and interest assessed by any taxing authority or municipality that arise from Customer's failure to pay any taxes or fees properly invoiced to Customer. In the event of any assessment by a taxing authority or municipality, both Parties agree to cooperate with each other to resolve issues in order to minimize such assessment. The Parties agree to cooperate to recognize and apply any applicable tax exemptions granted to Customer under State and local law.

6.3. Payment Terms. Customer shall pay all Fees by the date they are due as described in Schedule C.

7. PROPRIETARY RIGHTS

7.1. Work Product. As used herein, the term **"Work Product,"** which excludes Feedback (as defined below) and Meter Data, means all other materials, software, tools, data, inventions, works of authorship and other innovations of any kind, including any improvements or modifications to hardware, software and related materials, that DPL, or personnel working for or through DPL, may make, conceive, develop or reduce to practice, alone or jointly with others, in the course of performing DPL's responsibilities under this Agreement, whether or not eligible for patent, copyright, trademark, trade secret or other legal protection. Customer agrees that all Work Product shall be the sole and exclusive property of DPL and DPL' s suppliers. Customer hereby assigns all its rights, if any, in the Work Product and in all related patents, patent applications, copyrights, mask work rights, trademarks, trade secrets, rights of priority and other proprietary rights to DPL. Customer acknowledges that DPL, in its sole discretion, shall have the right to license the Work Product or any portion thereof, or incorporate the Work Product or any portion thereof into products or services, for use by other licensees of DPL. At DPL's request and sole expense, Customer shall assist and cooperate with DPL in all reasonable respects and shall execute documents and take further acts as reasonably requested by DPL to acquire, transfer, maintain and enforce patent, copyright, trademark, mask work, trade secret and other legal protection for the Work Product. Customer hereby unconditionally and irrevocably grants to DPL an assignment of all right, title, and interest in and to the Resultant Data, including all intellectual property rights relating thereto, provided the Resultant Data shall not be used, sold or assigned for any marketing uses or disclosed outside of DPL and its Affiliates except in aggregated format.

7.2. Feedback License. Each Party hereby grants to the other a perpetual, irrevocable, fully paid-up, royalty-free, transferable, sublicensable (through multiple levels of sublicensees), non-exclusive, worldwide right and license to use, reproduce, distribute, display and perform (whether publicly or otherwise), prepare derivative works of and otherwise modify, make, sell, offer to sell, import and otherwise use and exploit (and have others exercise such rights) all or any portion of the Feedback (as defined below), in any form or media (now known or later developed). As used herein, **"Feedback"** means reports and works of authorship, deliverables and data exchanged or provided under this Agreement, any and all suggestions, ideas, correction or enhancement requests, feedback, recommendations or other information relating to DPL's Network, any Work Product by or on behalf of one Party to the other Party or any of its employees, agents, Affiliates or contractors. For the sake of clarity and the avoidance of doubt, Feedback does not include Work Product or Meter Data.

7.3. Reservation of Rights. Except as otherwise expressly provided in this Agreement, nothing in this Agreement shall be deemed to grant, directly or by implication, estoppel or otherwise, any right or license with respect to any technology or other intellectual property rights, and each Party retains all right, title and interest in and to their respective technologies and other intellectual property rights.

7.4. Source Code Disclosures. If DPL discloses any source code to Customer in connection with this Agreement, such source code shall be subject to all of the obligations under Section 8 and the following additional restrictions on use and disclosure: (a) Customer shall allow use of or access to the source code only by Customer and its Affiliates and its and their employees, agents, and contractors who have a need to use the source code for exercise of Customer's rights with respect to the source code as set forth in this Agreement and who are bound to retain the confidentiality thereof under written non-disclosure agreements or policies that include provisions (including provisions relating to nonuse and nondisclosure) no less restrictive than those required under this Agreement; (b) Customer shall maintain and use the source code only in secure, locked facilities or on servers to

which access is limited to the Persons set forth in subsection (a), above; (c) for source code that is useable or stored on any computer equipment (whether a multi-user system, network, stand-alone computer or otherwise), the equipment must have password-based access control, with each user having a unique user identification and associated password; and (d) Customer shall maintain a record of the number of copies made, if any, of the source code, and the computer equipment and storage media on which the source code is used or stored.

7.5. License to Meter Data. For the Term of this Agreement, Customer hereby irrevocably grants all such rights and permissions in or relating to Meter Data as are necessary or useful to DPL to enforce this Agreement and exercise DPL's rights and perform DPL's obligations under this Agreement.

8. CONFIDENTIALITY

8.1. Confidentiality Obligations. In connection with this Agreement, each Party (the **"Disclosing Party"**) may disclose or make available Confidential Information to the other Party (the **"Receiving Party"**). The Receiving Party: (i) shall not disclose or otherwise make available Confidential Information of the Disclosing Party to any third party without the prior written consent of the Disclosing Party; *provided, however,* that the Receiving Party may disclose the Confidential Information of the Disclosing Party to its officers, employees, consultants, and legal advisors who have a "need to know", who have been apprised of this restriction, and who are themselves bound by nondisclosure obligations at least as restrictive as those set forth in this Section 8.1; (ii) shall use the Confidential Information of the Disclosing Party only for the purposes of performing its obligations or exercise its rights under the Agreement; and (iii) shall promptly notify the Disclosing Party if the Receiving Party becomes aware of any unpermitted disclosure of any of the Confidential Information of Disclosing Party.

8.2. Exceptions. Confidential Information does not include information that: (i) was rightfully known to the Receiving Party without restriction on use or disclosure prior to such information's being disclosed or made available to the Receiving Party in connection with this Agreement; (ii) was or becomes generally known by the public other than by the Receiving Party's noncompliance with this Agreement; (iii) was or is received by the Receiving Party on a non-confidential basis from a third party that was not or is not, at the time of such receipt, under any obligation to maintain its confidentiality; or (iv) was or is independently developed by the Receiving Party without reference to or use of any Confidential Information of the Disclosing Party.

8.3. Compelled Disclosures. If the Receiving Party becomes legally compelled to disclose any Confidential Information, including, but not limited to, comply with FOIA or the lawful order of a government authority, the Receiving Party shall provide: (i) prompt written notice by e-mail of such requirement so that the Disclosing Party may seek, at its sole cost and expense, a protective order or other remedy; and (ii) reasonable assistance, at the Disclosing Party's sole cost and expense, in opposing such disclosure or seeking a protective order or other limitations on disclosure. If, after providing such notice Receiving Party receives no reply from the Disclosing Party within five (5) business days, the Receiving Party shall disclose no more than that portion of the Confidential Information which, on the advice of the Receiving Party's legal counsel, the Receiving Party is legally required to disclose. If, after providing such notice Receiving Party receives within five (5) business days written notice by email from the Disclosing Party of its intent to oppose or limit such disclosure or seek a protective order, Receiving Party will provide reasonable assistance as required herein and, upon the Disclosing Party's request, shall use Commercially Reasonable Efforts to obtain assurances

from the applicable court or agency that such Confidential Information will be afforded confidential treatment. Notwithstanding anything in the foregoing to the contrary, the Receiving Party may disclose the Confidential Information if required to do so by the applicable court or agency. For the purpose of this Section 8.3, the notice required herein shall be addressed to a Party as follows (or to such other address or such other person that such Party may designate from time to time in accordance with this Section 8.3):

If to DPL:

If to Customer:

9. REPRESENTATIONS AND WARRANTIES

9.1. Mutual Representations and Warranties. Each Party represents and warrants to the other that: (i) it is a corporation validly existing and in active status under the Laws of the State of its incorporation; (ii) it has all the requisite corporate power and authority to execute, deliver and perform its obligations under this Agreement in accordance with its terms; (iii) the execution, delivery and performance of this Agreement has been duly authorized by it, and this Agreement is enforceable in accordance with its terms against it; (iv) it has obtained and shall maintain all licenses, authorizations and permits required to perform its obligations and exercise its rights under this Agreement under applicable Laws; and (v) it shall perform its obligations and exercise its rights under this Agreement in accordance with applicable Laws.

9.2. Disclaimer of Warranties. EXCEPT FOR THE EXPRESS WARRANTIES IN THIS SECTION 9, (A) EACH PARTY HEREBY DISCLAIMS ALL WARRANTIES, EITHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE UNDER THIS AGREEMENT, AND (B) DPL SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUSIVE OF THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT.

10. INDEMNIFICATION

10.1. Customer Indemnification of DPL. Customer shall indemnify, defend, and hold harmless DPL and its subcontractors and Affiliates, and each of its and their respective officers, directors, employees, agents, successors, and assigns (each, a **"DPL Indemnitee"**) from and against any and all Losses incurred by such DPL Indemnitee resulting from any Action by a third party (other than an Affiliate of a DPL Indemnitee) to the extent that such Losses arise out of or result from, or are alleged to arise out of or result from: (i) Meter Data, including any processing of Meter Data by or on behalf of DPL in accordance with this Agreement; (ii) Customer's failure to obtain any necessary consents or approvals as required under Section 3.3; (iii) allegation of facts that, if true, would constitute Customer's breach of any of its representations or warranties under this Agreement; or (iv) gross negligence or more culpable act or omission (including recklessness or willful misconduct) by Customer or any third party on behalf of Customer in connection with this Agreement. The Parties expressly acknowledge that that the foregoing indemnification provision shall not waive Customer's immunity derived from (i) the

County and Municipal Tort Claims Act set forth in Title 10, Chapter 40, Subchapter II of the Delaware Code or (ii) elsewhere.

10.2. DPL Indemnification of Customer. DPL shall indemnify, defend, and hold harmless Customer and its subcontractors and Affiliates, and each of its and their respective officers, directors, employees, agents, successors, and assigns (each, a **"Customer Indemnitee"**) from and against any and all Losses incurred by such Customer Indemnitee resulting from any Action by a third party (other than an Affiliate of a Customer Indemnitee) to the extent that such Losses arise out of or result from, or are alleged to arise out of or result from: (i) allegation of facts, if true, that the provision of the Services as provided by DPL constitutes infringement of any patent, copyright, trademark, trade secret or other proprietary right of such third party, (ii) allegation of facts that, if true, would constitute DPL' s breach of any of its representations or warranties under this Agreement, or (iii) gross negligence or more culpable act or omission (including recklessness or willful misconduct) by DPL or any third party on behalf of DPL in connection with this Agreement. Notwithstanding the immediately preceding sentence, DPL shall have no obligation to indemnify Customer for Losses arising out of or resulting from the use of the Headend Systems, any modifications to the Services made by or at the request of Customer, or any good, service, technology, or other matter (including any software, hardware, firmware, system, or network) provided by or on behalf of Customer or directed by Customer to be installed, combined, integrated, or used with, as part of, or in connection with the Services where such was not previously in use in connection with the Services, except for gross negligence or more culpable act or omission (including recklessness or willful misconduct) by DPL or any third party on behalf of DPL in connection with this Agreement.

10.3. Indemnification Procedures. The Party seeking indemnification hereunder (the **"Indemnified Party"**) shall promptly notify the other Party (the **"Indemnifying Party"**) in writing of any Action for which it seeks and the other Party is obligated to provide indemnification under this Section 10 (the **"Indemnified Claim"**) and cooperate with the Indemnifying Party at the Indemnifying Party's sole cost and expense. The Indemnifying Party shall immediately take control of the defense and investigation of such Indemnified Claim and shall employ counsel reasonably acceptable to the Indemnified Party to handle and defend the same, at the Indemnifying Party's sole cost and expense. The Indemnifying Party shall not settle any Indemnified Claim in a manner that adversely affects the rights of the Indemnified Party without the Indemnified Party's prior written consent, which shall not be unreasonably withheld or delayed. The Indemnified Party's failure to perform any obligations under this Section 10 shall not relieve the Indemnifying Party of its obligations under this Section 10 except to the extent that the Indemnifying Party can demonstrate that it has been materially prejudiced as a result of such failure. The Indemnified Party may participate in and observe the proceedings of an Indemnified Claim at its own cost and expense.

11. LIMITATION OF LIABILITY

11.1. Cap on Monetary Liability. In no event will the aggregate liability of either Party to the other Party arising out of or related to this Agreement, whether arising under or related to maintenance or equipment failure, network interruptions, breach of contract, tort (including negligence), strict

liability, or any other legal or equitable theory, exceed the amount of any insurance or self-insurance maintained by the respective Party which provides coverage related to such Losses or $1 million, whichever is less. The foregoing limitations apply even if any remedy fails of its essential purpose.

11.2. Exclusion of Certain Damages. Except as set forth in Section 11.3, in no event shall either Party be liable to the other for any Consequential or Special Damages, punitive, or exemplary damages even if such Party has been advised of the possibility of such potential loss or damage. For purposes of this Section 11.2, **"Consequential or Special Damages"** means remote or speculative damages or damages which are not the natural and probable result of a breach of this Agreement.

11.3. Exceptions. The exclusions and limitations in Section 11.1 and Section 11.2 do not apply to (i) either Party's obligation to pay amounts due under this Agreement; (ii) indemnification obligations under Section 10; (iii) liability for a Party's breach of Section 2.4, Section 7.4, or Section 8; (iv) liability resulting from a Party's gross negligence or more culpable act or omission (including recklessness or willful misconduct, bad faith, intentional misconduct, or fraud claims; (v) Customer's breach of its access and security obligations under Section 3.5 of this Agreement; or (vi) the obligations set forth in the attached Exelon (DPL's parent) Exhibit H.

12. FORCE MAJEURE

12.1. Generally. Neither Party shall be liable or responsible to the other Party, nor be deemed to have defaulted under or breached this Agreement, for any failure or delay in fulfilling or performing any term of this Agreement (except for any obligations to make payments to the other Party hereunder), when and to the extent such failure or delay is caused by or results from acts beyond the impacted Party's **("Impacted Party")** reasonable control, including without limitation the following force majeure events **("Force Majeure Events"):** (a) acts of God; (b) flood, fire, earthquake, epidemic, or explosion; (c) war, invasion, hostilities (whether war is declared or not), terrorist threats or acts, riot, or other civil unrest; (d) government order, Law, or actions; (e) embargoes or blockades in effect on or after the date of this Agreement; (f) national or regional emergency; and (g) strikes, labor stoppages or slowdowns, or other industrial disturbances. The Impacted Party shall give notice to the other Party promptly upon its failure or delay (or obtaining a reasonable belief that it will have a failure or delay) in fulfilling or performing any term of this Agreement resulting from a Force Majeure Event to the other Party, stating the nature of the Force Majeure Event and the period of time the failure or delay is expected to continue.

12.2. Efforts to Resolve Force Majeure. The Impacted Party shall use diligent efforts to end the failure or delay and to minimize the effects of a Force Majeure Event and shall resume performance of its obligations as soon as reasonably practicable after the removal of the cause or the development of a method to continue performance of its obligations despite the Force Majeure Event. If the Impacted Party's failure or delay remains uncured for a period of thirty (30) days following written notice given by it under this Section 12, the other Party may thereafter terminate this Agreement upon thirty (30) days' written notice.

13. GENERAL PROVISIONS

13.1. Relationship of the Parties. The relationship between the Parties is that of independent contractors. The details of the method and manner for performance of the Services by DPL shall be under its own control, Customer being interested only in the results thereof. DPL shall be solely responsible for supervising, controlling, and directing the details and manner of the completion of the

Services. Nothing in this Agreement shall give the Customer the right to instruct, supervise, control, or direct the details and manner of the completion of the Services. The Services must meet the Customer's final approval and shall be subject to the Customer's general right of inspection throughout the performance of the Services and to secure satisfactory final completion. Nothing contained in this Agreement shall be construed as creating any agency, partnership, joint venture or other form of joint enterprise, employment, or fiduciary relationship between the Parties, and neither Party shall have authority to contract for or bind the other Party in any manner whatsoever.

13.2. Public Statements. Except to the extent required by FOIA, neither Party shall issue or release any announcement, statement, press release, or other publicity or marketing materials relating to this Agreement, and neither Party shall, unless expressly permitted under this Agreement, otherwise use the other Party's trademarks, service marks, trade names, logos, or domain names, in each case, without the prior written consent of the other Party, which consent shall not be unreasonably withheld.

13.3. Notices. Except as otherwise expressly set forth in this Agreement, any notice, request, consent, claim, or demand under this Agreement have legal effect only if in writing and addressed to a Party as follows (or to such other address or such other person that such Party may designate from time to time in accordance with this Section 13.3):

If to DPL:

If to Customer:

Notices sent in accordance with this Section 13.3 will be deemed effectively given: (a) when received, if delivered by hand, with signed confirmation of receipt; (b) when received, if sent by a nationally recognized overnight courier, signature required; (c) when sent, if by facsimile or email, (in each case, with confirmation of transmission), if sent during the addressee's normal business hours, and on the next business day, if sent after the addressee's normal business hours; and (d) on the third (3rd) day after the date mailed by certified or registered mail, return receipt requested, postage prepaid.

13.4. Interpretation. For purposes of this Agreement: (i) the words "include," "includes," and "including" are deemed to be followed by the words "without limitation"; (ii) the word "or" is not exclusive; (iii) the words "herein", "hereof", "hereby", "hereto", and "hereunder" refer to this Agreement as a whole; (iv) comparable meaning when used in the plural, and vice-versa; and (v) words denoting any gender include all genders. Unless the context otherwise requires, references in this Agreement: (a) to sections, schedules, and attachments mean the sections of, and schedules and attachments attached to this Agreement; (b) to an agreement, instrument, or other document means such agreement, instrument, or other document as amended, supplemented, and modified from time to time to the extent permitted by the provisions hereof; and (c) to a statute means such statute as amended from time to time and includes any successor legislation thereto and any regulations promulgated thereunder. The Parties intend this Agreement to be construed without regard to any presumption or rule requiring construction or interpretation against the Party drafting an instrument

or causing any instrument to be drafted. The schedules and attachments referred to herein are an integral part of this Agreement to the same extent as if they were set forth verbatim herein.

13.5. Entire Agreement and Precedence. This Agreement, including and together with any related schedules and attachments, constitutes the sole and entire agreement of the Parties with respect to the subject matter contained herein, and supersedes all prior and contemporaneous understandings, agreements, representations, and warranties, both written and oral, regarding such subject matter. The Parties acknowledge and agree that if there is any conflict between the terms and conditions of the body of this Agreement and the terms and conditions of any schedule and attachment, the terms and conditions of the body of this Agreement shall supersede and control.

13.6. Assignment.

13.6.1 Customer shall not assign or otherwise transfer any of its rights, or delegate or otherwise transfer any of its obligations or performance under this Agreement, in each case whether voluntarily, involuntarily, by operation of law, or otherwise, without DPL's prior written consent, not to be unreasonably withheld, conditioned, or delayed. No assignment, delegation, or transfer will relieve Customer of any of its obligations or performance under this Agreement. Any purported assignment, delegation, or transfer in violation of this Section 13.6 is void. This Agreement is binding upon and inures to the benefit of the Parties hereto and their respective successors and permitted assigns.

13.6.2 DPL shall not assign or otherwise transfer any of its rights, or delegate or otherwise transfer any of its obligations or performance under this Agreement, in each case whether voluntarily, involuntarily, by operation of law, or otherwise, except to any of its Affiliates or with Customer's prior written consent, not to be unreasonably withheld, conditioned, or delayed. No assignment, delegation, or transfer will relieve DPL of any of its obligations or performance under this Agreement. Notwithstanding the foregoing, DPL may hire contractors and subcontractors to perform its obligations hereunder with the approval of Customer, not to be unreasonably withheld.

13.7. No Third-Party Beneficiaries. Except for Persons who are indemnified by a Party under Section 10, this Agreement benefits solely the Parties to this Agreement and their respective successors and permitted assigns and nothing in this Agreement, express or implied, confers on any other Person or entity any legal or equitable right, benefit, or remedy of any nature whatsoever under or by reason of this Agreement.

13.8. Headings. The headings in this Agreement are for reference only and do not affect the interpretation of this Agreement.

13.9. Modifications. No amendment to or modification of this Agreement is effective unless it is in writing, identified as an amendment to or rescission, termination, or discharge of this Agreement and signed by an authorized representative of each Party.

13.10. Waiver. No waiver by any Party of any of the provisions of this Agreement shall be effective unless explicitly set forth in writing and signed by the Party so waiving. Any waiver shall be effective only with respect to the exercise or performance of the particular right or obligation described in writing and shall not result in a waiver of any other act or omission. Except as otherwise set forth in this Agreement, no failure to exercise, or delay in exercising, any right, remedy, power, or privilege arising from this Agreement shall operate or be construed as a waiver thereof, nor shall any single or

partial exercise of any right, remedy, power, or privilege hereunder preclude any other or further exercise thereof or the exercise of any other right, remedy, power, or privilege.

13 .11. Severability. If any term or provision of this Agreement is found by a court of competent jurisdiction to be invalid, illegal, or unenforceable in any jurisdiction, such invalidity, illegality, or unenforceability shall not affect any other term or provision of this Agreement or invalidate or render unenforceable such term or provision in any other jurisdiction. Upon a determination that any term or provision is invalid, illegal, or unenforceable, the court may modify this Agreement to affect the original intent of the Parties as closely as possible in order that the transactions contemplated hereby be consummated as originally contemplated to the greatest extent possible.

13.12. Governing Law, Jurisdiction, and Forum. This Agreement and all related documents, and all Actions arising out of or relating to this Agreement, whether sounding in contract, tort, or statute are governed by, and construed in accordance with, the Laws of the State of Delaware, United States of America, without giving effect to the conflict of laws provisions thereof to the extent such principles or rules would require or permit the application of the Laws of any jurisdiction other than those of the State of Delaware. Each Party irrevocably and unconditionally agrees that it will not commence any Action against any other Party in any way arising from or relating to this Agreement and all contemplated transactions in any forum other than the United States District Court for the State of Delaware or, if such court does not have subject matter jurisdiction, the courts of the State of Delaware sitting in New Castle County, Delaware, and any appellate court from any thereof, and each Party consents to the exclusive jurisdiction of such courts for such Actions. Each Party agrees that a final judgment in any such Action is conclusive and may be enforced in other jurisdictions by suit on the judgment or in any other manner provided by law.

13.13. Informal Dispute Resolution. The Parties shall resolve any Action arising out of or relating to this Agreement (each, a **"Dispute"**), under the provisions of Sections 13 .12 through Section 13.15. The Parties shall first attempt in good faith to resolve any Dispute by negotiation and consultation between themselves beginning with negotiation sessions between a director of each Party (or other employee of similar seniority) (the **"Director Negotiations"**). If a Dispute is not resolved within thirty (30) days of the start of Director Negotiations, either Party may, by written notice to the other Party (**"Escalation to Executive Notice"**), refer such Dispute to an executive-level employee of each Party (with each Party to select its executive-level employee in its sole discretion) for negotiation. If the Parties cannot resolve a Dispute within fourteen (14) days after the date of the Escalation to Executive Notice, either Party may initiate a claim as permitted under Section 13.12.

13.14. Waiver of Jury Trial. Each Party irrevocably and unconditionally waives any right it may have to a trial by jury in respect of any Action arising out of or relating to this Agreement or the transactions contemplated hereby.

13.15. Equitable Relief. Each Party acknowledges and agrees that a breach or threatened breach by such Party of any of its obligations under Section 8 or, in the case of Customer, Section 2.4 or Section 3.5 would cause the other Party irreparable harm for which monetary damages would not be an adequate remedy and that, in the event of such breach or threatened breach, the other Party will be entitled to equitable relief, including a restraining order, an injunction, specific performance, and any other relief that may be available from any court located in New Castle County, Delaware, without any requirement to post a bond or other security, or to prove actual damages or that monetary

damages are not an adequate remedy. Such remedies are not exclusive and are in addition to all other remedies that may be available at law, in equity, or otherwise.

13.16. Itron Agreement. The Parties acknowledge that (a) Customer will execute an agreement with Itron, Inc. (the "**Itron Agreement**"), (b) the Itron Agreement provides the Customer with hardware and firmware which is required to facilitate DPL's provision of the Services, and (c) DPL's Network relies on compatible hardware and firmware also provided by Itron. The Parties agree that the Customer, Itron, and DPL will work together in good faith to jointly plan, schedule, and approve of any software or firmware improvements, patches or releases by Itron.

13.17 Counterparts. This Agreement may be executed in counterparts, each of which is deemed an original, but all of which together are deemed to be one and the same agreement. A signed copy of this Agreement delivered by facsimile, email, or other means of electronic transmission is deemed to have the same legal effect as delivery of an original signed copy of this Agreement.

13.18 Insurance Coverage. DPL shall provide insurance coverage for itself and all of its employees, if any, used in connection with this Agreement as follows: workers' compensation as required by law and commercial general liability coverage for personal injury, including death, and property damage in the minimum amount of One Million Dollars ($1,000,000.00). Such policies shall be issued by a financially sound carrier and/or carriers and shall be subject to the reasonable approval of Customer. DPL shall provide Customer with a certificate of insurance evidencing the above-stated coverage and naming Customer as an additional insured.

13.19 Discrimination and Harassment. In the performance of this Agreement, the Parties agree that they shall not discriminate or harass, or permit discrimination or harassment, against any individual because of age, sex, marital status, race, religion, color, national origin or sexual orientation.

13.20 Records. DPL shall maintain accounts and records, including personnel, property, and financial records, adequate to identify and account for all costs pertaining to this Agreement and such other records as may be deemed necessary by Customer to assure proper accounting for all project funds. Such records shall be made available for audit purposes to Customer or its authorized representatives upon request.

13.21 Reports and Information. DPL, at such time and in such form as Customer may require, shall furnish Customer such reports as Customer may request pertaining to the Services undertaken pursuant to this Agreement.

13.22 System and Organization Control Reports. DPL shall maintain and upon request provide to Customer any and all System and Organization Control Reports (also known as Service Organization Control Reports) ("**SOC Reports**") DPL has acquired that are related to DPL's business. Customer shall treat all SOC Reports as Confidential Information and shall not disclose any SOC Report to a third party, except that disclosure shall be permitted to the City's internal and external auditors, attorneys, and other advisers. Notwithstanding the foregoing, if the City receives a request under FOIA for documents that include a SOC Report, the City shall follow the procedures set forth in Section 8.3 of this Agreement.

13.23 Business License. DPL shall obtain and/or maintain an appropriate business license from the City of Wilmington Department of Finance.

13.24 Taxes. DPL shall withhold, if applicable, City of Wilmington wage taxes from the compensation of its officers, agents and employees as required by the City of Wilmington wage tax law.

13.25 Findings Confidential. All of the drawings, plans, designs, reports, analyses, specifications, information, examinations, proposals, illustrations, copies, maps, graphics, slides, and documents prepared, assembled, drafted, or generated by DPL under this Agreement are Confidential Information subject to the provisions of Section 8.1 of this Agreement.

[Remainder of this page left blank.]

IN WITNESS WHEREOF, the Parties have caused this Agreement to be signed by their respective officers thereunto duly authorized all as of the date first written above.

DELMARVA POWER & LIGHT COMPANY

_____

Name: David Vosvick, VP Smart Meter Operations

_____

Date

CITY OF WILMINGTON

_____

Name

_____

Date

SCHEDULE A

DESCRIPTION OF SERVICES

Startup Period

The Parties shall work together to complete the milestone activities described in the table below (each, a **"Milestone"**) on or prior to the date listed in the column titled "Target Completion Date" for such Milestone (the **"Target Completion Date"**).

Following the Parties' agreement that a Milestone is ready for testing, the Parties shall work together to test the Milestone based upon the criteria set forth in the column titled "Acceptance Criteria" for such Milestone (the **"Acceptance Criteria"**).

Following the completion of testing for the Acceptance Criteria for a particular Milestone, the Parties shall: (i) agree that the Acceptance Criteria have been met and the Parties can move to the following Milestone or the Steady-State Services (defined below); or (ii) agree upon any failures of the Milestone to meet the Acceptance Criteria (each, a **"Non-Conformity"**) and a plan for further development and testing to resolve the Non-Conformities. If the Parties identify any Non-Conformities, the Parties shall work together to remedy all such Non-Conformities and re-test the relevant Milestone against the Acceptance Criteria as promptly as commercially possible.

#	Milestone Activity	Acceptance Criteria	Target Completion
1	End-to-end testing in production environment with <100 Provisioned Endpoints • Validate end-to-end system functionality and data flow • Validate deployment and provisioning processes • Validate hard to reach endpoint mitigation processes	Test plan completed and results documented and approved by the Parties	February 2026
2	Steady-State Services	Completion of Milestones 1 and 2	April 2026

The Start Up Period shall be from the Effective Date of the Agreement until the commencement of Steady-State Services, as defined below.

Steady-State Services

Beginning upon the completion of Milestones 1 and 2, DPL shall provide the following services to Customer (the **"Steady-State Services"):**

• Enable the connection of Provisioned Water Meters to DPL's AMI Mesh Network

• Transmit water meter data from Provisioned Water Meters via the Network to Customer's Headend System

• Make available to Customer a daily data set that includes daily register data, hourly interval data, and event data for each Provisioned Water Meter

• Investigate and identify issues preventing accurate or consistent data transmission from the Network Devices as described below:

o Remotely investigate and resolve issues - 2nd level triage including identifying the last proxy device, verifying network availability, and identifying Network Devices to be replaced

o Conduct in-field RF investigations as needed - 3" level triage including in-field inspections as necessary if there is an issue with a Network Device

o NOTE: Itron performs Level 1 triage

• Provision of a testing environment and reasonable testing resources in which new Headend System versions and new Network Devices and Water Meters and associated firmware may be tested.

Within five (5) business days of a request from DPL, Customer shall provide DPL with a report that includes the following information: (i) Provisioned Water Meters installed during the period request by DPL; (ii) Provisioned Water Meters removed during the period request by DPL; (iii) Provisioned Water Meters (or the interface management unit for such Provisioned Water Meters) exchanged during the period request by DPL; (iv) accurate geographical coordinates for each Provisioned Water Meter; and (v) Provisioned Water Meters (or the interface management unit for such Provisioned Water Meter) permanently destroyed.

Each month during the Term and the Startup Period and within sixty (60) days following the end of the Startup Period, Customer shall provide DPL with a written report certified by an independent third party or ITRON related to the destruction and sanitization of the interface management units in Provisioned Water Meters that includes, at a minimum: (i) the vendor providing the report, (ii) the sanitization process used (e.g., NIST 800-88), and (iii) the serial number or MAC address for each interface management unit.

If the Customer has completed its investigation of an Instance of Unavailability and determined that Provisioned Water Meter or part thereof need to be replaced or repaired to resolve such issue, then Customer shall be responsible for repairing or replacing such Provisioned Water Meter or part thereof. DPL shall have no liability for its failure to provide Services with regard to any such Provisioned Water Meter until it has been repaired or replaced by Customer.

If DPL has completed its investigation of an Instance of Unavailability and determined that the issue is resulting from the inability of a particular Provisioned Water Meter to connect to DPL' s AMI Mesh Network because of inadequate strength of the radio frequency signals, the Parties shall discuss in

good faith the appropriate resolution. If the Parties agree that the appropriate resolution is to install a different endpoint on a Provisioned Water Meter (e.g., a remote wired device), then Customer will bear the cost of such resolution. If the Parties agree that the appropriate resolution is to strengthen the DPL's AMI Mesh Network in the relevant area (e.g., by installing an external antenna on an electrical meter, installing a relay), then DPL will bear the cost of such resolution.

System Upgrades

Each Party will provide at least twelve (12) months' advance written notice to the other Party prior to upgrading its Headend System. Upon receiving or providing such notice, DPL will perform testing to ensure that the Headend System as upgraded is compatible with the Services, and Customer will perform testing to ensure that the Headend System as upgraded is capable of integrating with Customer's systems. The Parties will work together in good faith to address any issues arising out of an upgrade to either Party's Headend System including, if continuation of the Services is not commercially reasonable after such upgrade, terminating the Agreement as described in Section 5.5 of the body of the Agreement.

Customer will provide DPL with at least three (3) calendar days' advance written notice before upgrading the firmware on any of its Provisioned Water Meters. DPL shall conduct testing to ensure compatibility of the upgraded firmware with the Services including functional testing and compatibility testing with DPL's Headend System. Customer shall cooperate with DPL in working with Customer's and DPL's Headend System vendor to schedule production firmware upgrades as necessary. The Parties will work together in good faith to address any issues arising out of an upgrade to either Party's device firmware including, if continuation of the Services is not commercially reasonable after such upgrade, terminating the Agreement as described in Section 5.5 of the body of the Agreement.

SCHEDULE B

AVAILABILITY COMMITMENT

DPL shall maintain an availability percentage of 99% average daily read rate for each Measurement Period other than during scheduled downtime for disaster recovery exercises and other maintenance purposes (the "**Availability Commitment**")

- The DPL AMI Network SLA applies to the network communications performance from the electric meter up to where the water meter is talking through the electric meter, APs, Relays & photocells

- This SLA does not include the performance of Customer's water meter communicating with the electric meter, to the extent that DPL's AMI network is available as defined above, Customer is responsible for the performance of the water meter communicating with the AMI Network and any associated network only troubleshooting (e.g., if it's not communicating with an available network). Network troubleshooting does not include meters.

- DPL AMI Network SLA performance of 99% will be based on the average daily network availability over a billing month, determined as follows:

    - DPL's "Automated Meter Infrastructure (AMI) Mesh Network" for this Agreement will include devices including DPL smart meters, Access Points (APs), and Relays within the Customer's territory servicing residential, commercial and industrial customers

    - These devices shall be considered "available" if they successfully transmit electric meter usage via DPL's AMI communications protocols occurring three (3) times per day

    - DPL will generate reports showing daily availability performance during a billing month indicating the average daily availability

No Provisioned Water Meter will be included in the calculation of Availability under this Agreement unless it is fully powered and actively communicating with a Network Device on DPL's AMI Mesh Network for at least seven consecutive days prior to the point at which Availability is measured.

DPL shall have no liability for failure to meet the Availability Commitment for any Measurement Period in which there are fewer than one thousand (1,000) Provisioned Water Meters.

For the avoidance of doubt, the Availability Commitment does not apply to the performance of Water Meters or the communications between any Water Meter and a Network Device.

Beginning at the start of the first calendar month following the start of Steady-State Services, DPL shall issue a monthly report reflecting DPL's performance with respect to the Availability Commitment for the prior month.

SCHEDULE C

Year	Annual Fee		
2026	$91,200	Annual Fee due on 6/1/26	Based on 38,000 endpoints
2027	$93,936	Annual Fee due on 6/1/27	
2028	$96,754	Annual Fee due on 6/1/28	
2029	$99,657	Annual Fee due on 6/1/29	
2030	$102,646	Annual Fee due on 6/1/30	
2031	$105,726	Annual Fee due on 6/1/31	
2032	$108,898	Annual Fee due on 6/1/32	
2033	$112,164	Annual Fee due on 6/1/33	
2034	$115,529	Annual Fee due on 6/1/34	
2035	$118,995	Annual Fee due on 6/1/35	
2036	$122,565	Annual Fee due on 6/1/36	
2037	$126,242	Annual Fee due on 6/1/37	
2038	$130,029	Annual Fee due on 6/1/38	
2039	$133,930	Annual Fee due on 6/1/39	
2040	$137,948	Annual Fee due on 6/1/40	
	$1,696,221		

SCHEDULE D

See attached Exelon's EXHIBIT H – BASIC CYBER AND INFORMATION SECURITY SPECIAL TERMS AND CONDITIONS

EXHIBIT H – BASIC CYBER AND INFORMATION SECURITY SPECIAL TERMS AND CONDITIONS

ARTICLE 1 - SCOPE

1.1 If Contractor and its Subcontractors will access, process, store or transmit Buyer's Electronic Confidential Information on Contractor's or Subcontractor's Electronic Information Assets, they will adhere to the requirements of this Exhibit H.

1.2 Contractor and its Subcontractors will adhere to the requirements in both this Exhibit H and Exhibit L (Advanced Cyber and Information Security Special Terms and Conditions) if they will use Contractor's or Subcontractor's Electronic Information Assets to: (1) access, process, store, transmit or transform Buyer Electronic Restricted Confidential Information; (2) access Buyer Electronic Information Assets using Remote Access Systems; (3) have a Direct Network Connection to Buyer's Electronic Information Assets; (4) provide Digital Materials for installation on or connection to Buyer's Electronic Information Assets; (5) perform Digital Services on Buyer's Electronic Information Assets and Digital Materials that will be installed on or connected to them; (6) provide Cloud Computing Services to Buyer which access, process, store or transmit Buyer's Electronic Restricted Confidential Information; or (7) connect to Buyer BES Cyber System using Contractor's or Subcontractors' Removable Media or Transient Cyber Asset.

1.3 Exhibit H does not apply to Contractors or its Subcontractors who access, process, store or transmit Buyer's Electronic Confidential Information, or perform Digital Services, exclusively on and using Buyer-provided Electronic Information Assets and who are governed by the Exelon Acceptable Use Policy, SY-AC-6.

ARTICLE 2 - DEFINITIONS

Capitalized terms not defined herein will have the meaning given to them elsewhere in the Terms and Conditions.

"Acceptable Use Policy" means a policy that defines the security requirements, prohibitions, and expected behaviors required of all Buyer personnel, contractors, and third-party personnel, including suppliers, that have been granted authorized access to Buyer facilities, assets, systems, or information.

"**Account ID**" means any identification name or code associated with an Electronic Information Asset account (e.g. Administrator Account IDs, Service Account IDs, Shared Account IDs, System Account IDs and User Account IDs) that provides a specific level of access.

"Administrator Account" means an account with elevated privileges that allows users to make changes that affect other Users or configuration settings (e.g. copy and paste information, change security settings, install software and hardware, access all files on a system or make changes to other user accounts).

"Affiliate" means Persons that, directly or indirectly, now or hereafter, own or control, are owned or controlled by, or are under common ownership or control of the company at issue, where "control" means at least a fifty percent (50%) ownership interest

"**Application**" means a software program or collection of integrated software programs that supports a business function, and any Security Patches or upgrades thereto, including electronic data processing, information, recordkeeping, communications, telecommunications, account management, inventory management, and internet websites.

"Artificial Intelligence" means a machine-based Electronic Information Asset that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual Electronic Information Assets. Artificial Intelligence uses machine and human-based inputs to (a) perceive real and virtual Electronic Information Assets; (b) abstract such perceptions into models through analysis in an automated manner; and (c) use model inference to formulate options for information or action.

"Back Door" means methods for bypassing computer authentication in the procured Materials or Services.

"BES" means the bulk electric system (as designated by NERC).

"BES Cyber Asset" means Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation, or non-operation, adversely impact one or more facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System (as defined by NERC).

"BES Cyber System" means one or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity (as defined by NERC).

"BES Cyber System Information" is a category of Restricted Confidential Information and means information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, Electronic Security Perimeter names, or policy statements. Examples of BES Cyber System Information include security procedures or security information about BES Cyber Systems, physical access control systems, and electronic access control or monitoring systems that are not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System (as defined by NERC).

"**Business Continuity Plan**" means a documented strategy outlining the steps and processes to ensure your business operations continue to run should disaster strike.

"Buyer" means Exelon or the Affiliate that issues a particular Purchase Order.

"Buyer Data" means any data, documents or information in whatever media: (a) provided to Contractor by Buyer; (b) provided to Contractor by a third-party contractor of Buyer, customer of Buyer or other Person designated by Buyer ; or (c) sent by Contractor to a third-party contractor of Buyer, customer of Buyer or other Person designated by Buyer in connection with the Work, including images of bills and invoices, telephone call recordings, records of solicitations, and other correspondence.

"CEII" is a category of Restricted Confidential Information that consists of both **"Critical Electric Infrastructure Information"** and **"Critical Energy Infrastructure Information"** as each are defined by the FERC regulations in 18 CFR §388.113(c). Critical Electric Infrastructure Information is designated by FERC or the Secretary of the Department of Energy pursuant to Section 215A(d) of the Federal Power Act and similar information, even if not designated by FERC or the Secretary of the Department of Energy, and includes information that qualifies as Critical Energy Infrastructure Information, which includes specific engineering, vulnerability, or design details 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 (FOIA); (d) gives strategic information beyond the general location of the critical infrastructure; and (e) "Critical Electric Infrastructure Information" as defined in Fixing America's Surface Transportation Act, Pub. L. No. 114-94 § 61,003 (to be codified at 16 U.S.C. § 824 et seq.), 18 C.F.R. §§ 388.112-113.

"Cloud Computing Services" means the delivery of computing services over the Internet, including servers, storage, databases, networking, software, analytics, and intelligence. It includes IaaS, PaaS, SaaS, and serverless Applications (where the cloud service provider automatically provisions, scales, and manages the infrastructure required to run the code).

"Compromise" means any circumstance where information or assets have been accessed, acquired, corrupted, damaged, destroyed, disclosed, lost, modified, used, or otherwise endangered by any unauthorized Person, by any person in an unauthorized manner, or for an unauthorized purpose.

"Confidential Information" means: all information disclosed by or on behalf of a Party, regardless of the form or medium contained or stored in (including hard copy, electronic, or digital form), that is: (1) marked or identified as "confidential," "proprietary," or with words of similar import; (2) is required by Law or by agreement to be maintained as confidential, including Customer Information, Energy Usage Data when combined with Customer Information, State Regulated Information, and Third Party Confidential Information; (3) not generally available to the trade or public and that may be of competitive or economic value to the owner, including Background Investigation reports, business methods, business plans, credit report information, financial information, Intellectual Property, labor negotiations, legal documents, market research, marketing strategies and techniques, outage schedules, operations and operational requirements, payroll information, personnel information, plant status, policies and procedures, pricing data and price lists, proposals for Materials and Services; prospect lists, and contact information, research software, technical information and technology; and (4) Restricted Confidential Information. Confidential Information will include any such information not generally available to the trade or public, even though such information has been previously disclosed to one or more third parties pursuant to confidentiality agreements, disclosure agreements or other agreements or collaborations entered into by the disclosing Party.

"Contract Documents" means the Purchase Order, any Change Orders thereto, these Terms and Conditions, and any other documents identified as Contract Documents herein, or in such Purchase Order or Change Orders.

"Contractor Information Security Program" means a program comprised of security policies, standards, procedures and controls designed to protect the integrity, availability, and confidentiality of Buyer's Electronic Confidential Information and Electronic Information Assets, including phishing, Malware, and social engineering attacks.

"Contractor" means the Party identified as such in these Terms and Conditions or its Affiliate, which is named in the Purchase Order as Contractor and which is contractually responsible to perform the Work pursuant to the Purchase Order incorporating these Terms and Conditions.

"Contractor Personnel" means any and all individuals assigned by, through or on behalf of Contractor or its Subcontractors to perform the Work, including their partners, employees, officers, and agents.

"Customer Information" is a category of Confidential Information and means information supplied to Buyer by its residential, commercial, industrial, retail and wholesale customers

"Cyber Assets" Programmable electronic devices, including the hardware, software, and data in those device (as defined by NERC).

"Cyber Security Incident" means any act or event, or a group of events occurring during the performance of, or in connection with the Work, that is a Compromise, or has or had the potential to be a Compromise, of: (1) BES Cyber Systems Electronic Security Perimeters or Physical Security Perimeters; (2) BES Cyber System operations; (3) Buyer's Electronic Information Assets, (4) Buyer's Electronic Confidential Information stored or transmitted on Contractor's Electronic Information Assets; (5) the operation of Buyer's business, (6) Digital Materials or Digital Services provided or performed by Contractor; or (7) violates a cyber security or information security requirement in the Contract Documents, Cyber Security Laws or Policies and Procedures, including when:

(a) Contractor knows or reasonably believes that there has been a Compromise of BES Cyber Systems Electronic or Physical Security Perimeters or operations;

(b) Contractor knows or reasonably believes that there has been a Compromise of Buyer Electronic Information hosted or stored by Contractor;

(c) Contractor knows or reasonably believes that there has been a Compromise of the cybersecurity of the Digital Materials and Services provided to Buyer by Contractor;

(d) Contractor knows or reasonably believes that there has been a Compromise of the physical, technical, administrative, or organizational safeguards protecting either Contractor's or Buyer's Electronic Information Assets accessing, processing storing or transmitting Buyer Electronic Confidential Information or Restricted Confidential Information;

(e) Contractor receives any complaint, notice, or communication that relates directly or indirectly to:

(i) Contractor's handling of Buyer's Electronic Information;

(ii) Contractor's compliance with the cyber security or information security requirements in these Terms and Conditions or applicable Cyber Security Laws or Policies and Procedures in connection with Buyer's Electronic Information; or

(iii) the cybersecurity of the Digital Materials and Services provided to Buyer by Contractor or

(f) Contractor, in the exercise of reasonable care as determined by industry best practices, should have discovered a Compromise of Buyer's Electronic Information.

"Cyber Security Incident Management Process" means a process to identify, manage, record, analyze and remediate cyber or physical security threats or Cyber Security Incidents.

"Cyber Security Laws" means any Laws pertaining to the prevention and reporting of Cyber Security Incidents, including Cybersecurity Act of 2015 (P.L. 114-113), Cybersecurity Enhancement Act of 2014 (P.L. 113-2), Economic Espionage Act of 1996 (18 U.S.C. § 1030, §§ 1831-39).

"**Data-At-Rest**" means Electronic Information which is stored physically in any electronic form (e.g. databases, data warehouses, spreadsheets, archives, tapes, off-site backups, mobile devices etc.).

"Data Backup Plan" means a plan which establishes processes and procedures to duplicate and maintain Buyer Electronic Information and allow retrieval of the duplicate set of data after a data loss event.

"**Data-In-Transit**" means Electronic Information that is transmitted over the public or untrusted network such as the internet and data which flows in the confines of a private network such as a corporate or enterprise Local Area Network (LAN).

"**Digital Materials**" means Applications, Firmware, System Software, and Material that contain or utilize a programmable electronic device (including micro-processors and micro-controllers) or the operation of which is capable of being electronically accessed via the Internet or Wi-Fi.

"**Digital Services**" means the assembly, design, development, manufacture, modification, repair, servicing, or testing of Digital Materials or Buyer's Electronic Information Assets; and the digital delivery and hosting of Services, including Cloud Computing Services.

"Disaster Recovery Plan" means a disaster recovery plan set forth in Article 13 (Disaster Recovery and Business Continuity).

"Electronic Confidential Information" means Electronic Information which is Confidential Information or Restricted Confidential Information.

"**Electronic Information**" means any information accessed, processed, stored or transmitted in an electronic format (e.g., emails, text messages, raw data, sound files, image files, video files, documents, spreadsheets, databases, programs and algorithms).

"**Electronic Information Assets**" means any electronic device or system for creating, processing, storing, transmitting or receiving Electronic Information, including but not limited to computers (e.g., laptops, desktops), computer Applications, System Software, computer systems hardware (e.g., servers and routers), voicemail, facsimile (fax), printers, copiers, telephone, recording devices; portable devices (e.g., smart phones, tablets), wireless routers, electronic mail, web pages, modems, internal computer network and external computer access (e.g. systems accessing the Internet, intranet, value add networks and bulletin boards).

"**Electronic Security Perimeter**" means the logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol (as defined by NERC).

"**Encryption**" means the process of converting information or data into a code designed to prevent unauthorized access.

"**Energy Usage Data,**" commonly known as interval data, is a category of Confidential Information and means a series of measurements of the energy consumption for a specific customer, taken at regularly spaced intervals. The size of the interval refers to the amount of time that occurs between each measurement (i.e. monthly, daily, hourly, etc.).

"**Export Controlled Information**" is a category of Restricted Confidential Information and includes information required to be protected pursuant the applicable Laws relating to the exportation of commodities or technical data and economic and trade sanctions, including but not limited to: 15 CFR Parts 730 et seq., 10 CFR Part 110, and 10 CFR Part 810, 15 CFR Parts 700-799, and the U.S. Office of Foreign Assets Control Sanctions Lists, as issued from time to time, or any successor Laws.

"**Firmware**" means a software program or set of instructions programmed on a hardware device, and any Security Patches or upgrades thereto. It provides the necessary instructions for how the device communicates with the other hardware devices.

"**IaaS**" or "**Infrastructure as a Service**" means an instant computing infrastructure, provisioned and managed over the internet.

"**Law**" or "**Laws**" means all laws, statutes, codes, ordinances, rules, regulations, lawful orders, applicable guidance documents from regulatory agencies, judicial decrees and interpretations, standards, requirements, permits and licenses; including Cyber Security Laws, Environmental Laws, Health and Safety Laws, Privacy and Consumer Protection Laws, tax laws and applicable tax treaties, building, labor and employment laws; as amended from time to time, of all Governmental Authorities that are applicable to the Work and any of Contractor's obligations under the Contract Documents.

"**Malware**" means a form of unauthorized, hostile or intrusive software code or programming instruction(s) intentionally designed to disrupt, disable, harm, monitor, interfere with or otherwise adversely affect computer programs, data files or operations (excluding software keys), including adware, Back Doors, botnets, key loggers, ransomware, rootkits, spyware, Trojan horses, viruses, worms and other types of disabling, harmful, malicious, or unauthorized computer code, files, links, content, scripts, messages, agents, or programs.

"**Material**" means all components, equipment, goods, hardware, parts, products, raw materials, supplies, systems and related documentation to be furnished by Contractor as set forth in the Purchase Order or required to complete the Work, and includes Digital Materials.

"**Material Business Information**" is a category of Restricted Confidential Information and means non-public information of the Buyer or its Affiliates that would be considered important by a reasonable investor in deciding whether

to buy, sell or hold securities of the Buyer or its Affiliates, and includes information could reasonably be expected to affect the price of the Company's securities if it were disclosed to the public; information concerning earnings estimates or targets, dividends, proposals or agreements for significant mergers, acquisitions or divestitures, liquidity or litigation problems, important management changes, pending regulatory actions and other similar events.

"NERC" means the electric reliability organization known as the North American Electric Reliability Corporation or its successor, or a regional reliability organization with authority delegated by NERC, including the ReliabilityFirst Corporation, Northeast Power Coordinating Council, Florida Reliability Coordinating Council, Midwest Reliability Organization, SERC Reliability Corporation, Southwest Power Pool, RE, Texas Regional Entity, and the Western Electricity Coordinating Council.

"NERC CIP Information" is a category of Restricted Confidential Information and means NERC Critical Infrastructure Protection operational procedures, lists as required in NERC Standard CIP-003-3, network topology or similar diagrams, floor plans of computing centers that contain BES Cyber Assets, equipment layouts of BES Cyber Assets, disaster recovery plans, incident response plans, and security configuration.

"PaaS" or "Platform as a Service" means a complete development and deployment environment in the cloud, with resources that enable Buyer to deliver everything from simple cloud-based apps to sophisticated, cloud-enabled enterprise Applications.

"Personally Identifiable Information" or **"PII"** is a category of Restricted Confidential Information and means any name, number, or other information that may be used, alone or in conjunction with any other information, to identify, distinguish, trace or assume the identity of a specific person, including any: (1) names, initials, mother's maiden name, address, email address, password, account number, social security number, date of birth, official state or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, or any similar identification; (2) personal, financial, or healthcare information; (3) credit and debit card information, bank account number, credit card number or debit card number; (4) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation, (5) unique electronic identification number, address, or routing code; (6) telecommunication identifying information or access device as defined in 18 U.S.C. §1029(e); or (7) personal preferences, demographic data, marketing data; (8) "Nonpublic Personal Information," as defined under the Gramm-Leach-Bliley Act (15 U.S.C. §6801 et seq.); (9) "Protected Health Information" as defined under the Health and Insurance Portability and Accountability Act of 1996 (42 U.S.C. §1320d); (10) "Personal Data" as that term is defined in EU Data Protection Directive (Directive 95/46/EEC) on the protection of individuals with regard to processing of personal data and the free movement of such data; or (11) any other similar identification data.

"Physical Security Controls" mean policies, standards and procedures designed to prevent unauthorized physical access, damage, and interference to Buyer Electronic Information and Assets.

"Physical Security Perimeter" means the physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled (as defined by NERC).

"Privacy and Consumer Protection Laws" mean Laws pertaining to privacy and confidentiality of consumer information, PII, consumer protection, and advertising, whether in effect now or in the future and as they may be amended from time-to-time, including the Gramm-Leach-Bliley Act of 1999 (Public Law 106-102, 113 Stat. 1138), the Fair and Accurate Credit Act of 2003, and Telephone Consumer Protection Act of 1991 (Public Law 102-243).

"Production System" means computer system used to process an organization's daily work or a system or environment with which Users interact.

"Purchase Order" means a written or electronic document issued by Buyer to Contractor incorporating by reference these Terms and Conditions and which upon acceptance by Contractor creates a contract for the performance of the Work. As used herein, the term Purchase Order includes documents that may be variously referred to as "contracts," "orders," "releases," or "statements of work (SOWs)," or names of similar import.

"Real Time Industrial Control Systems Information" is a category of Restricted Confidential Information and means information regarding the configuration or protection of real-time industrial control systems.

"Remote Access Systems" mean Applications that allow a User to connect to a computer network from a remote location, such as Citrix and VPN.

"Restricted Confidential Information" is a subset of Confidential Information and includes: (1) attorney-client privileged communications and attorney work product of Buyer; (2) BES Cyber System Information (3) CEII; (4) Material Business Information; (5) NERC CIP Information; (6) Personally Identifiable Information; (7) Real-Time Industrial Controls Systems Information; (8) Safeguards Information; (9) security plans involving both physical and cyber assets; (10) SUNSI; (11) Transmission Function Information; (12)Export Controlled Information; (13) information marked "for your eyes only," "for internal use only," "reproduction or distribution prohibited", or marked with similar restrictions (14) and other information that is protected by Law or Policies and Procedures that requires the highest level of access control and security protection.

"**SaaS**" or **"Software as a Service"** means a software distribution model in which Contractor manages and provides to the Buyer over the Internet all aspects of the software solution and environment, including the underlying infrastructure, middleware, Application, and data.

"Safeguards Information" is a category of Restricted Confidential Information and means information relating to (1) security measures for the physical protection of special nuclear material; and (2) security measures for the physical protection and location of certain plant equipment vital to the safety of nuclear power stations as set forth in 10 C.F.R. Section 73.2.

"Security Asset Lifecycle Program" means a program comprised of policies, standards, procedures, and controls which define the development, implementation, maintenance, review and monitoring of ownership, inventory, return, and acceptable uses of Buyer Electronic Information and Assets.

"Security Controls" mean safeguards or countermeasures to avoid, detect, counteract or minimize security risks to Buyer physical property, Electronic Information or Assets.

"**Security Patch Management**" means identifying, acquiring, analyzing, and testing Security Patches, as well as planning, communicating, implementing, and verifying their deployment.

"**Security Patches**" mean a software or computer system patch that is intended to correct a Vulnerability in that software or system.

"**Service Account**" means an account used for servicing a computer system that may be used by more than one User. This account may be a system account where Users cannot log into the account, but would know the account's credential/password to change this credential/password.

"**Shared Account ID**" means an Account ID shared between two or more Users.

"State-Regulated Information" is a category of Confidential Information and means information that is not generally available to the public that is related to either (1) Buyer's or its Affiliates' customers or (2) transmission and distribution systems, as further defined in various state Laws.

"SUNSI" or **"Sensitive Unclassified Non-Safeguards Information"** is a category of Restricted Confidential Information and has the definition given to it by the NRC and includes information about a licensee's or applicant's physical protection for special nuclear material not otherwise designated as Safeguards Information or classified as National Security Information or Restricted Data that is required by 10 CFR 2.390.

"**System Software**" means software programs that run in the background, enabling Applications to run, and any Security Patches or upgrades thereto, including assemblers, compilers, file management tools, and the operating system itself.

"Third-Party Confidential Information" is a category of Confidential Information and means information that is owned by a third party and is disclosed to the Buyer with the requirement that it will be kept confidential.

"Transmission Function Information" is a category of Restricted Confidential Information and means information related to non-public transmission data, including information about available transmission capability, price, curtailments and/or ancillary services.

"**User**" means any Person able to access an Electronic Information Asset.

"**VPN**" means a virtual private network which extends a private network across a public network or internet and enables Users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

"Vulnerability or Vulnerabilities" means one or more weakness or material defect in the design, manufacture or operation of an Application, System Software, Digital Material, Digital Service, or Electronic Information Asset that could result in a Compromise, including manual configuration and operational mistakes (including bad passwords); insider malfeasance; functional bugs; purposefully introduced Malware; general weaknesses in code; and Back Doors.

"Work" means all Material, Services, and Submittals required to be provided by Contractor under the Purchase Order and its associated Contract Documents, including re-work and warranty work.

ARTICLE 3 - CONTRACTOR'S INFORMATION SECURITY PROGRAM

3.1 Contractor will document, implement, and maintain a Contractor Information Security Program to protect the integrity, availability, and confidentiality of Buyer's Electronic Confidential Information in accordance with the requirements set forth in this Exhibit H.

3.2 Contractor will train Contractor Personnel with access to Buyer Electronic Confidential Information on the key elements of the Contractor Information Security Program so that they understand their responsibilities for the secure handling of Buyer's Electronic Confidential Information.

3.3 Contractor will provide annual information security awareness refresher training to Contractor Personnel who have access to Buyer's Electronic Confidential Information. Training will include Contractor's Information Security Program and standards for the secure handling of Buyer's Electronic Confidential Information.

3.4 Contractor will include as part of its information security program anti-phishing protections via an email security platform or application specifically designed to detect and prevent phishing attempts (e.g. Ironscales, Mimecast, Barracuda, INKY, etc.) and will train Contractor Personnel to recognize signs of phishing in company emails.

ARTICLE 4 - CONTRACTOR'S ACCESS MANAGEMENT PROGRAM

4.1 Contractor will only grant access to Contractor's Electronic Information Assets where Buyer Electronic Confidential Information is processed, stored, or transmitted to Contractor Personnel who need access to perform the Work and will revoke such access promptly once the Person no longer requires or is no longer qualified for access.

4.2 Contractor will assign each individual Contractor Personnel a unique User Account ID for which Contractor will be responsible for all activities performed under that User Account ID.

4.3 Contractor will limit Administrator Account access to Buyer Electronic Confidential Information being processed, stored or transmitted using Contractor's Electronic Information Assets to only those Contractor Personnel whose job role and responsibilities require such access. Contractor will revoke such access promptly once the Contractor Personnel no longer requires access, is no longer qualified for access or is no longer working for the Contractor.

4.4 Contractor will ensure that Administrator, Shared, and Service Account ID passwords are changed as soon as possible upon an assigned User's notification of termination or change in job role that no longer requires such access.

4.5 Contractor will prohibit Contractor Personnel to share or otherwise allow other Persons to use their unique User Account IDs and associated passwords and terminate access to Buyer Electronic Confidential Information for Contractor Personnel who violate this prohibition.

4.6 Contractor will promptly remove Contractor Personnel's access to any Buyer Electronic Confidential Information and Contractor Electronic Information Assets where Buyer Electronic Confidential Information is stored when: (i) the individual no longer requires access to a given Electronic information resource or Electronic Information Asset; or (ii) when Contractor reasonably believes the individual may pose a threat to the safety or security of Buyer's Electronic Confidential Information.

4.7 Where the Contractor allows Contractor Personnel to use personal devices to access or transmit Buyer Electronic Confidential Information processed, stored, or transmitted in Contractor's Electronic Information Assets, the Contractor will implement an Acceptable Use Policy and Security Controls commensurate with the sensitivity of the Buyer Electronic Confidential Information.

ARTICLE 5 - CONTRACTOR DATA BACKUP OF BUYER ELECTRONIC CONFIDENTIAL INFORMATION

5.1 Contractor will develop, implement, maintain, review and monitor a Data Backup Plan to protect the confidentiality, integrity, and availability of Buyer's Electronic Confidential Information.

5.2 The Data Backup Plan will include a regular data backup schedule, identification of an offsite location where data backups are held in an encrypted/secure form, a prompt data restoration timeframe, and an appropriate testing schedule to confirm the data plan is effective.

ARTICLE 6 - CONTRACTOR'S USE OF CRYPTOGRAPHY

6.1 Contractor will utilize IPS 140-2 compliant cryptographic protocols.

6.2 Contractor will encrypt Buyer Electronic Confidential Information while Data-at-Rest or Data-in-Transit, including authentication credentials and cryptographic keys.

ARTICLE 7 - CONTRACTOR'S CYBER SECURITY INCIDENT REPORTING, RESPONSE & RECOVERY

7.1 Contractor will document, implement, and maintain a Cyber Security Incident Management Process to protect the confidentiality, integrity and availability of Buyer's Electronic Confidential Information.

7.2 Contractor's Cyber Security Incident Management Process will be comprised of security policies and procedures designed to identify, manage, record, analyze, and execute proper response to Cyber Security Incidents or Cyber Threats.

7.3 Contractor will immediately inform Buyer upon becoming aware of any Cyber Security Incident.

7.4 Contractor will promptly, but in no case more than 24 hours from discovery, provide a verbal report of any Cyber Security Incidents to the Exelon Security Operations Center by telephone (to 1-800-550-6154, international at 410-470-5800), and follow up by email (to ESOC@exeloncorp.com). The report will include the date and time of the occurrence of the Cyber Security Incident (or the approximate date and time of the occurrence if the actual date and time of the Cyber Security Incident is not precisely known) and a detailed summary of the facts and circumstances of the Cyber Security Incident, including a description of (a) why the Cyber Security Incident occurred, and (b) the measures being taken to address and remedy the Cyber Security Incident to prevent the same or a similar event from occurring in the future. Contractor will provide written updates of the notice to Buyer addressing any new facts and circumstances learned after the initial written notice of a Cyber Security Incident is provided and will provide such updates within a reasonable time after learning of those new facts and circumstances. Where the Cyber Security Incident involves Digital Services supplied by the Contractor, this notification requirement will continue for so long as Contractor provides the Digital Services supplied to Buyer or, in the case of licensed Digital Services, for so long as Buyer licenses the Digital Services.

7.5 Within ten (10) days of notifying Buyer of the Cyber Security Incident, Contractor will recommend actions to be taken by Buyer to reduce the risk of a recurrence of the same or a similar Cyber Security Incident, including, as appropriate, the provision of action plans and mitigating controls. Contractor will coordinate with Buyer in developing those action plans and mitigating controls. Contractor will provide Buyer guidance and recommendations for long-term remediation of any cyber security risks posed to Buyer Electronic Confidential Information and Buyer Electronic Information Assets, as well as any information necessary to assist Buyer in any recovery efforts undertaken by Buyer in response to the Cyber Security Incident.

7.6 Contractor will investigate all incidents and provide Buyer a written report detailing the known and unknown facts of the incident, continuing to provide such report until Contractor and Buyer agree the incident should be considered closed.

7.7 Contractor will not publicly disclose any unauthorized access to Buyer's Electronic Confidential Information or any breach of Buyer's Electronic Information Assets without Buyer's prior written consent, unless Contractor is required to do so by applicable Law.

ARTICLE 8 - CONTRACTOR'S SECURITY PATCH MANAGEMENT

8.1 Contractor will have Security Patch Management procedures that require prompt application of Security Patches to System Software, Applications and Electronic Information Assets in a consistent, standardized and prioritized manner based upon criticality and risk. If a Security Patch cannot be promptly applied due to requirements for testing, then effective risk mitigation controls will be implemented until such time as Security Patches can be applied.

8.2 Contractor will provide a Security patch or fix as soon as possible, but in no event later than sixty (60) days from the notification of such Vulnerability or risk.

8.3 Contractor will test all Security Patches on systems that accurately represent the configuration of the target Production Systems before deployment of the patch to Production Systems and that the correct operation of the patched system is verified after any patching activity.

8.4. Contractor will promptly notify Buyer's Designated Representative of any Vulnerability that cannot be effectively closed by a Security Patch or other corrective action by Contractor and will document and implement appropriate mitigating technical controls to protect Buyer's Electronic Confidential Information.

ARTICLE 9 - CONTRACTOR'S PASSWORD MANAGEMENT

9.1 Contractor will ensure that Contractor's Electronic Information Assets which access, process, store, or transmit Buyer's Electronic Confidential Information employ strong password complexity rules.

9.2 Contractor will require all Contractor Personnel to comply with Contractor's password requirements.

9.3 Passwords will be at least eight (8) characters long and composed of lower and upper-case letters, numbers and special characters (where special characters are technically feasible). If special characters are not used, passwords will be at least twelve (12) characters long.

9.4 Contractor will ensure automatic logoff or locking is implemented and enforced, requiring all users to log in to regain access if they have been inactive for a pre-determined period of time, which, as a minimum, should be no longer than 15 minutes of inactivity.

9.5 Contractor will require Contractor Personnel to change passwords for access to Contractor's Electronic Information Assets, which access, process, store, or transmit Buyer's Electronic Confidential Information, at reasonable intervals, but in any event, no less than once per year or as required by industry standards.

9.6 Contractor will deny access to Contractor's Electronic Information Assets, which access, process, store, or transmit Buyer's Electronic Confidential Information, if a user unsuccessfully attempts to log into these accounts.

ARTICLE 10 - CONTRACTOR'S PHYSICAL SECURITY

10.1 Contractor will implement, manage, and review appropriate Physical Security Controls to prevent unauthorized physical access to Contractor's Electronic Information Assets or Buyer's Electronic Confidential Information stored on them.

10.2 Contractor will ensure its Electronic Information Assets in which Buyer's Electronic Confidential Information are stored are appropriately secured from unauthorized physical access.

10.3 Contractor will maintain all backup and archival media containing Buyer's Electronic Confidential Information in secure, environmentally controlled storage areas owned, operated, or contracted for by Contractor.

10.4 Contractor will have processes and procedures for the control and monitoring of visitors' and other external persons' physical access to Contractor's Electronic Information Assets on which Buyer's Electronic Confidential Information is stored, including its own contractors with physical access to secure areas for the purpose of environmental control, maintenance, alarm maintenance and cleaning.

ARTICLE 11 - CONTRACTOR'S MALWARE PROTECTION

11.1 Contractor will deploy industry-standard Malware protection software on all its Electronic Information Assets that access, process, store or transmit Buyer's Electronic Confidential Information.

11.2 Contractor will ensure Malware protection technology has the latest and up-to-date manufacturer's signatures, definition files, software, and Security Patches.

ARTICLE 12 - CYBER SECURITY INCIDENT / NETWORK SECURITY INSURANCE

Contractor will provide and maintain Cyber Security Incident/Network Security Insurance with a limit of not less than five million dollars ($5,000,000) per occurrence and in the aggregate. Coverage will include liability for financial loss resulting from or arising out of acts, errors, or omissions in the performance of contractual obligations assumed by Contractor under the Contract Documents, including: (i) breaches of Buyer's information security Policies and Procedures; (ii) violation of any right to privacy or privacy Laws; (iii) Cyber Security Incidents and violation of any Cyber Security Laws; (iv) data theft, damage, destruction, or corruption, including unauthorized access, unauthorized use, identity theft, theft of Personally Identifiable Information or confidential corporate information, transmission of a computer virus or other type of malicious code; and (v) denial or loss of service attacks, including ransomware attacks; (vi) Internet advertising and content offenses; (vii) defamation; (viii) errors or omissions in software or systems development, implementation and maintenance. Such insurance will address all of the foregoing, without limitation, if caused by Contractor or Subcontractor in performing the Services or Work under the Contract Documents. Policy will provide coverage for wrongful acts, claims, and lawsuits anywhere in the world and cover data breach costs and expenses, whether or not required by applicable Law or otherwise.

ARTICLE 13 - DISASTER PREPAREDNESS AND BUSINESS CONTINUITY

13.1 Contractor will document, implement, and maintain a Business Continuity Plan to protect the privacy, confidentiality, integrity, and availability of Buyer's Electronic Information, Electronic Information Assets, and Digital Materials.

13.2 The Business Continuity Plan shall include an appropriate data backup schedule, identification of an offsite location where data backups are held in an encrypted/secure form, a prompt data restoration timeframe, and an appropriate testing schedule to confirm the Business Continuity Plan is effective.

13.3 Contractor Business Continuity Plan will include back-up, disaster recovery and storage capabilities so as to maximize availability and progress of the Work during an event that would otherwise affect the performance or delivery of the Work. At a minimum, such capabilities will provide for restoration of Work within the timeframes set forth in the Disaster Recovery Plan. Contractor's responsibilities will include the following:

13.3.1 Contractor will back-up and store Buyer Data (on tapes or other storage media as appropriate) on-site for efficient data recovery and off-site to provide protection against disasters and to meet file recovery needs.

13.3.2 Contractor will encrypt Buyer Data when being transmitted or stored outside of Buyer's computer systems and network. Buyer Data will be classified according to Buyer's required levels of classification.

13.3.3 Contractor will conduct incremental and full back-ups (in accordance with the Disaster Recovery Plan) to capture data, and changes to data used in connection with the Work. Backed up data will be encrypted.

13.3.4 Contractor will develop, maintain and make available to Buyer a Disaster Recovery Plan to Buyer including plans, measures and arrangements to ensure the continuous delivery of critical products and services, which permits Contractor to recover its facility, data, assets and personnel.

13.3.4.1 In the event of a disaster, Contractor will assume responsibility for providing the services in accordance with the Disaster Recovery Plan.

13.3.4.2 Contractor will generate a report following each and any disaster measuring performance against

the Disaster Recovery Plan and identification of problem areas and plans for resolution.

13.3.5 Contractor's Business Continuity Plan documentation will be made available to Buyer upon request.

ARTICLE 14 - USE OF GENERATIVE AI

Contractor will not input, insert, use, share, or transmit any Buyer's Confidential Information within any generative Artificial Intelligence software, Applications, tool, equipment or platform for any purposes, without first receiving Buyer's express written consent.