bge
AN EXELON COMPANY

CONFIDENTIALITY, NON-DISCLOSURE, AND TERMS OF USE AGREEMENT

THIS CONFIDENTIALITY, NON-DISCLOSURE, AND TERMS OF USE AGREEMENT (this "Agreement") dated _____ is entered into by and between _____ (the "Recipient") and Baltimore Gas and Electric Company (the "Company"). The Company and the Recipient shall be referred to collectively as the "Parties" and individually as a "Party". This Agreement governs the use of Confidential Information, including BGE Information (as defined in Section 1(a) below) and Critical Energy Infrastructure Information ("CEII") (as such term is more fully defined in Exhibit 1) disclosed by the Company, its parent entity(ies) or its other affiliates, and/or any of their respective officers, employees, agents, contractors, consultants, insurers, attorneys, or representatives (collectively, "Company Representatives") to the Recipient and any of its officers, employees, or any independent contractors meeting the requirements of Section 2(c) (collectively, "Recipient Representatives") for the Purpose specified in Section 1(c) below during the Term of this Agreement.

The Parties to this Agreement hereby agree as follows:

1. Definitions

(a) The term "BGE Information" refers to confidential, proprietary, and security sensitive information and data related to electric, gas, communication, and other facilities owned, leased, operated, maintained, or otherwise controlled by BGE, including, but not limited to, any such information and data concerning the location of such facilities. The term "BGE Information" also refers to any such information that is classified as CEII.

(b) The term "Confidential Information" refers to all BGE Information and any other information or data that the Recipient has access to under this Agreement. For the avoidance of any doubt, the term "Confidential Information" shall also include any document, analysis, report, or compilation prepared by the Company, the Recipient, or any other party that contains BGE Information or any other information or data that the Recipient has access to under this Agreement, which is not otherwise available to the public or the Company's competitors, whether disclosed orally or in writing at any time and whether made available to or observable by the Recipient and Recipient Representatives in any form or media (including hard copy, electronic, digital form or through access to any data room), including both the existence and contents of this Agreement. The term "Confidential Information" also includes, without limitation, the existence of the discussions between the Parties concerning the Purpose, and any proposed terms and the status of the Purpose and all Confidential Information obtained by the Recipient or Recipient Representatives prior to the execution of this Agreement.

(c) The term "Purpose" refers to the manner in which the Recipient and Recipient Representatives shall use the Confidential Information, which for purposes of this Agreement shall be described as follows:

_____
_____
_____
_____.

2. Disclosure and Use of Confidential Information

(a) The Company shall provide the Recipient with access to certain Confidential Information requested by the Recipient that relates to the Purpose.

(b) The Recipient will retain any Confidential Information in strictest confidence and will not use, exploit, or disclose, or permit the use, exploitation, or disclosure of, any Confidential Information, except as specified in this Agreement. The Recipient's and Recipient Representatives' use of any Confidential

Information shall be restricted only to the Purpose, and access to the Confidential Information shall be limited to the Recipient and Recipient Representatives with a need for access to the Confidential Information. The Recipient shall take all necessary and appropriate measures to ensure that any officer or employee who is granted access to any Confidential Information understands the terms of this Agreement and agrees to comply with such terms.

(c) The Recipient shall not disclose any Confidential Information to any other party without the Company's express prior written consent to do so; provided, however, the Recipient may disclose Confidential Information to any independent contractor retained by the Recipient in connection with the Purpose with a need for access to the Confidential Information that has executed an Acknowledgment and Acceptance of Confidentiality, Non-Disclosure, and Terms of Use Agreement in the form attached to this Agreement as Appendix A (the "Acknowledgment"). The Recipient shall deliver the executed Acknowledgment to the Company within five (5) calendar days of receipt.

(d) The Recipient will be responsible for any breach or anticipated breach of this Agreement by any Recipient Representatives or any third party to whom the Recipient or any Recipient Representative discloses Confidential Information.

(e) The Recipient's obligations under this Agreement do not apply to any portion of the Confidential Information that: (a) is or becomes publicly available by other than unauthorized disclosure; (b) is independently developed by the Recipient; or (c) is required to be produced by order of a court or other legitimate authority, provided that the Recipient first complies with the requirements of Section 9 of this Agreement.

(f) Notwithstanding anything to the contrary set forth in this Agreement, and provided that the Recipient complies with the requirement set forth in Section 2(e)i of this Agreement, the Recipient shall be permitted to disclose the following limited information obtained from Confidential Information to any government agency, client, government agency or client consultants, or third-party contractor performing work in connection with the Purpose, and such disclosure shall not be considered a violation of this Agreement, so long as such government agency, client, government agency or client consultants, or third-party contractor is informed of the confidential nature of such Confidential Information and agrees to maintain the confidentiality thereof:

_____

_____

_____

_____.

i. Any drawing, print, electronic file, or other document produced by the Recipient that contains the limited information listed in Section 2(f) shall also include the following written statement:

THIS DOCUMENT INCLUDES CONFIDENTIAL INFORMATION AND DEPICTIONS OF BALTIMORE GAS AND ELECTRIC COMPANY'S ("BGE") ELECTRIC AND/OR GAS UTILITIES LOCATED WITHIN THE PROJECT AREA (THE "BGE UTILITY INFORMATION"). LOCATIONS, DIMENSIONS, DEPTHS, AND OTHER DETAILS OF ANY SUCH UTILITIES MAY NOT BE AS-BUILT, AND THE INFORMATION SHALL NOT BE RELIED UPON WITHOUT FIELD VERIFICATION. EXCAVATORS MUST EMPLOY SAFE DIGGING BEST PRACTICES WHEN APPROACHING BGE ELECTRIC AND GAS UTILITIES AND COMPLY WITH ALL APPLICABLE FEDERAL, STATE, AND LOCAL LAWS, INCLUDING, BUT NOT LIMITED TO, THE "MISS UTILITY DIG LAW." NO REPRESENTATIONS, GUARANTEES, OR WARRANTIES, EXPRESS OR IMPLIED, ARE MADE BY BGE AS TO THE QUALITY,

COMPLETENESS, OR ACCURACY OF THE BGE UTILITY INFORMATION, AND IN ACCEPTING THIS DOCUMENT, THE RECIPIENT EXPRESSLY ACKNOWLEDGES AND AGREES THAT IT IS NOT RELYING ON THE ACCURACY OF THE SAME AND WILL MAINTAIN THE CONFIDENTIALITY OF THIS DOCUMENT .

3. Security of Confidential Information

The Recipient shall establish and implement systems, policies, practices, and protocols to secure and protect the Confidential Information from being disclosed to unauthorized individuals. Specifically, (i) in receiving Confidential Information under this Agreement, the Recipient will comply with the requirements of Exhibit 1 (Basic Cyber and Information Security Special Terms and Conditions) attached hereto and made a part hereof, and (ii) in receiving BGE Information that includes CEII, which the Recipient receives and/or stores electronically, the Recipient will also comply with the requirements of Exhibit 2 (Advanced Cyber and Information Security Special Terms and Conditions) attached hereto and made a part hereof.

4. Indemnification

To the fullest extent permitted by law, the Recipient shall indemnify, defend, and hold harmless the Company and its directors, officers, employees, agents, and representatives from and against any and all claims, losses, damages, demands, liabilities, and expenses, including reasonable attorneys' fees and costs, arising from or occurring in connection with any breach of this Agreement or any improper use or disclosure of the Confidential Information by the Recipient, Recipient Representatives, or Recipient's directors, agents, representatives, and contractors.

5. Warranty Disclaimer; No License

Confidential Information is provided on an "As-Is" basis. **NO REPRESENTATIONS, GUARANTEES, OR WARRANTIES, EXPRESS OR IMPLIED, ARE MADE BY THE COMPANY AS TO THE QUALITY, COMPLETENESS, OR ACCURACY OF ANY CONFIDENTIAL INFORMATION PROVIDED TO THE RECIPIENT, AND THE RECIPIENT EXPRESSLY AGREES THAT IT IS NOT RELYING ON THE ACCURACY OF THE SAME.** All Confidential Information shall remain the exclusive property of the Company. Nothing contained in this Agreement will be construed as granting or conferring any rights by license or otherwise in any Confidential Information disclosed to the Recipient or Recipient Representatives or in any intellectual property rights related thereto.

6. Compliance with Legal Requirements

The Recipient specifically acknowledges that the availability and use of the Confidential Information in no way relieves the Recipient of any and all obligations required by the "Miss Utility Dig Law" (Md. Code Ann., Public Utilities Art., Title XII, §§ 12-101 *et seq.*) and any other applicable laws, regulations, or standard industry practices. Recipient further acknowledges that any deficiencies or inaccuracies contained in the Confidential Information, whether real or alleged, may not be offered as a defense to any claim or cause of action of any kind.

7. Suspension and Termination of Access; Termination of the Agreement; Completion of Project; Return or Destruction of Confidential Information

(a) The Company shall have the right to immediately suspend or terminate access to the Confidential Information at any time, and upon the written request of the Company, the Recipient shall immediately return any Confidential Information to the Company and shall provide a certification in writing to the Company at the notice addresses set forth in Section 10(h) that all Confidential Information has been

permanently eliminated from the Recipient's electronic and other records or otherwise destroyed, with the limited exception set forth in Section 7(d).

(b) The Company shall have the right to terminate this Agreement for cause immediately upon written notice to the Recipient. Either Party may terminate this Agreement, with or without cause, upon thirty (30) calendar days' prior written notice to the other Party. Promptly upon termination of the Agreement for any reason the Recipient shall return all Confidential Information to the Company and shall provide a certification in writing to the Company at the notice addresses set forth in Section 10(h) that all Confidential Information has been permanently eliminated from the Recipient's electronic and other records or otherwise destroyed, with the limited exception set forth in Section 7(d).

(c) Within ten (10) calendar days after completion of any projects or tasks for which Confidential Information was provided under this Agreement, the Recipient shall (i) provide written notice of such completion to the Company, (ii) return all Confidential Information to the Company, and (iii) provide a certification in writing to the Company, all at the notice addresses set forth in Section 10(h), that all Confidential Information has been permanently eliminated from the Recipient's electronic and other records or otherwise destroyed, with the limited exception set forth in Section 7(d).

(d) The Recipient is not required to eliminate or destroy electronic copies of materials or summaries containing or reflecting Confidential Information to the extent maintained in the ordinary course of the Recipient's business and consistent with its record retention policy or that are automatically generated through data backup and/or archiving systems and are not readily accessible by Recipient's business personnel. In any event, the Recipient will maintain confidentiality of Confidential Information for the duration of its retention.

(e) Termination of this Agreement for any reason shall not release either Party from any rights, liabilities, or obligations set forth in this Agreement which by their nature should survive termination, including, but not limited to, the Recipient's obligations of security, confidentiality, and indemnification.

8. Remedies

The Recipient acknowledges, understands, and agrees that a breach of the terms, covenants or conditions contained in this Agreement will cause irreparable damage to the Company for which a remedy at law may be inadequate. Therefore, in the event of such breach or threatened breach, the Company shall be entitled to seek appropriate injunctive relief to enforce the terms of this Agreement and to prevent further use of any information improperly obtained or disclosed, in any court of competent jurisdiction, in addition to any other remedies available to it at law or in equity, and the Recipient hereby waives, and will cause Recipient Representatives to waive, any requirement for the securing or posting of any bond or other security in connection with any such remedy. This provision does not limit the Company's rights to seek monetary damages in addition to injunctive relief.

9. Legal Proceedings; Information Requests

(a) The Confidential Information may not be used by the Recipient for purposes of prosecuting or defending any claim involving the Company, the Recipient, or any other party, and the Confidential Information may not be used or disclosed in litigation unless procured from the Company by lawful process.

(b) The Recipient agrees to institute no claims, charges, suits, actions or appeals against or otherwise involving the Company, or any of Company Representatives, relating to matters arising out of or involving Confidential Information disclosed pursuant to this Agreement.

(c) The Recipient agrees that the Recipient will notify the Company in writing within five (5) calendar days of the receipt of any subpoena, court order, administrative order or other legal process requiring disclosure of Confidential Information; and that prior to responding to any such legal process, the Recipient shall provide written notice to the Company and provide the Company with the opportunity to file a motion to quash the subpoena and/or take other appropriate action to protect confidentiality and enforce the terms of this Agreement. The Recipient shall not oppose, and will cooperate with the Company and its counsel in the Company's efforts to prevent or limit the disclosure of Confidential Information, including filing of a motion to quash, a motion for protective order and/or other similar motions, and under no circumstances shall the Recipient or its attorneys disclose such Confidential Information unless and until they are compelled to do so by the order of a court or unless the Company consents to the disclosure.

(d) The Recipient agrees that the Recipient will notify the Company in writing within fifteen (15) calendar days of the receipt of any written request under the Maryland Public Information Act which requires disclosure of Confidential Information. The Company shall have the opportunity to comment to the Recipient about the written request under such Act and file a motion and/or other filing in court to protect the disclosure of Confidential Information. The Recipient shall not oppose the Company's filing of a motion and/or other appropriate action to protect the confidentiality of Confidential Information, but the Recipient shall respond to the written request according to such Act.

10. <u>Miscellaneous Terms and Conditions</u>

(a) The terms of this Agreement are severable and, as such, if any provision of this Agreement is held by a court of competent jurisdiction to be invalid, void, or unenforceable, the remaining provisions shall nevertheless continue in full force and effect without being impaired or invalidated .

(b) The Parties recognize, acknowledge, and agree that the failure by either Party to enforce any term of this Agreement shall not constitute a waiver of any rights or deprive either Party of the right to insist thereafter upon strict adherence to that or any other term of this Agreement, nor shall a waiver of any breach of this Agreement constitute a waiver of any preceding or succeeding breach. No waiver of any of the provisions of this Agreement shall be valid and binding unless it is in writing and signed by the Party against whom it is sought to be enforced.

(c) This Agreement shall be binding upon and shall inure to the benefit of the successors and assigns of the Parties hereto. The Recipient shall not assign any part of this Agreement without the written consent of the Company.

(d) This Agreement shall be construed in accordance with the laws of the State of Maryland without respect to any conflicts of law principles. The Parties agree that the federal and state courts sitting in the City of Baltimore will have exclusive personal jurisdiction over all Parties and any action involving a dispute under this Agreement will have as its venue a court located in the City of Baltimore and agree not to commence any action, suit or proceeding relating thereto except in such courts, and further agrees that service of any process, summons, notice or document by U.S. registered mail or by express courier such as Federal Express to a Party's address set forth below will be effective service of process for any action, suit or proceeding brought against a Party in any such court. Each Party hereby irrevocably and unconditionally waives any objection to the laying of venue of any action, suit or proceeding arising out of this Agreement or the transactions contemplated hereby in the courts located in the City of Baltimore, and hereby further irrevocably and unconditionally waives and agrees not to plead or claim in any such court that any such action, suit or proceeding brought in any such court has been brought in an inconvenient forum. THE PARTIES HERETO SPECIFICALLY WAIVE ANY RIGHT TO A JURY TRIAL WITH RESPECT TO ANY MATTER ARISING UNDER OR RELATED TO THIS AGREEMENT.

(e) It is expressly understood that this Agreement contains the entire agreement and supersedes any previous agreement, written or oral, between the Parties relating to the subjects contained herein and contains the entire and only agreement between the Parties respecting this subject matter. This Agreement may only be modified in writing, signed by both Parties.

(f) This Agreement may be executed by the Parties in two or more identical counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument. Signatures to this Agreement may be in any electronic or graphic form intended as a signature by the signatory and the document containing such signatures may be transmitted by electronic mail in PDF form or by any other electronic means intended to preserve the original graphic and pictorial appearance of a document, and in such form will have the same effect as physical delivery of a paper document bearing an original signature.

(g) The undersigned certify that they are authorized to execute this Agreement on behalf of their respective companies.

(h) Any notice provided for or permitted under this Agreement will be in writing and sent via email (receipt acknowledged), registered or certified mail (postage prepaid), or by commercial overnight courier, to the Party to be notified at the address set forth below, or at such other place of which the other Party has been notified in accordance with the provisions of this section. Notices will be effective only when received.:

FOR THE RECIPIENT:

Name:_____
Position:_____
Address:_____
_____
Email:_____

FOR THE COMPANY:

Name:_____
Position:_____
Address: 1068 Front St.
Baltimore, MD 21202
Email:_____

With a copy to:

Attn. General Counsel
Baltimore Gas and Electric Company
2 Center Plaza -13th Floor
110 West Fayette Street
Baltimore, Maryland 2120l
legalnotices@exeloncorp.com

[SIGNATURE PAGE FOLLOWS]

IN WITNESS WHEREOF, the Parties hereto have executed this Agreement.

	BALTIMORE GAS AND ELECTRIC COMPANY
Signature:_____	Signature:_____
Name:_____	Name:_____
Title:_____	Title:_____
Execution Date:_____	Execution Date:_____

APPENDIX A

ACKNOWLEDGMENT AND ACCEPTANCE OF CONFIDENTIALITY, NON-DISCLOSURE, AND TERMS OF USE AGREEMENT

The undersigned individual, _____, is the _____ of _____ ("Contractor"), which is located at _____, and is duly authorized to execute this Acknowledgement and Acceptance of Confidentiality, Non-Disclosure, and Terms of Use Agreement entered into between Baltimore Gas and Electric Company and Contractor dated _____ (the "Agreement") on behalf of the Contractor.

The Contractor is responsible for performing work in connection with the "Purpose'', as that term is defined in the Agreement. The Contractor acknowledges and confirms that it has been provided with a copy of the Agreement, and in consideration for the right to access certain "Confidential Information", as defined in the Agreement, the Contractor agrees to be bound by and abide by all of the terms, requirements, and conditions set forth in the Agreement applicable to the "Recipient", as defined in the Agreement.

Signature:_____

Execution Date:_____

EXHIBIT 1 – BASIC CYBER AND INFORMATION SECURITY SPECIAL TERMS AND CONDITIONS

ARTICLE 1 - SCOPE

1.1 If Recipient and Recipient Representatives will access, process, store or transmit Exelon's Electronic Confidential Information on Recipient's or Recipient Representatives' Electronic Information Assets, they will adhere to the requirements of this Exhibit 1.

1.2 Recipient and Recipient Representatives will adhere to the requirements in both this Exhibit 1 and Exhibit 2 (Advanced Cyber and Information Security Special Terms and Conditions) if they will use Recipient's or Recipient Representatives' Electronic Information Assets to: (1) access, process, store or transmit Exelon Electronic Restricted Confidential Information; (2) access Exelon Electronic Information Assets using Remote Access Systems; (3) have a Direct Network Connection to Exelon's Electronic Information Assets; (4) perform Digital Services on Exelon's Electronic Information Assets or (5) connect to Exelon BES Cyber System using Contractor's or Subcontractors' Removable Media or Transient Cyber Asset.

1.3 Exhibit 1 does not apply to Contractors or its Subcontractors who access, store or transmit Exelon's Electronic Confidential Information, or perform Digital Services, exclusively on and using Exelon-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 Agreement.

"Acceptable Use Policy" means a policy that defines the security requirements, prohibitions, and expected behaviors required of all Exelon personnel, contractors, and third-party personnel, including suppliers, that have been granted authorized access to Exelon 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, 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. change security settings, install software and hardware, access all files on a system or make changes to other user accounts).

"Agreement" means the Confidentiality and Nondisclosure Agreement to which this Exhibit 1 is attached.

"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.

"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.

"CEII" or **"Critical Energy Infrastructure Information"** is a category of Restricted Confidential Information as defined by FERC (18 CFR 388.113(c)(1)), and 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); and (d) gives strategic information beyond the location of the critical infrastructure; and **"**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" has the meaning set forth in Section 1 of the Agreement.

"Customer Information" is a category of Confidential Information and means information supplied to Exelon 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 malicious act or suspicious event, or group of suspicious events occurring when accessing, processing, storing or transmitting Exelon's Electronic Restricted Confidential Information, 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) Exelon's Electronic Information Assets, (4) Exelon's Electronic Confidential Information stored or transmitted on Recipient's Electronic Information Assets; (5) the operation of Exelon's business; or (6) violates a cyber security or information security requirement in Cyber Security Laws or Policies and Procedures, including when:

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

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

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

(d) Recipient receives any complaint, notice, or communication that relates directly or indirectly to:

(i) Recipient's handling of Exelon's Electronic Information; or

(ii) Recipient's compliance with the cyber security or information security requirements in this Agreement or applicable Cyber Security Laws or Policies and Procedures in connection with Exelon'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 Exelon 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 Exelon's Electronic Information Assets; and the digital delivery and hosting of Services, including Cloud Computing Services.

"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.).

"Exelon", for purposes of Exhibits 1 and 2, means Exelon Corporation and its subsidiaries, as applicable, including the Company.

"Exelon Data" means any data, documents or information in whatever media: (a) provided to Recipient by Exelon or Exelon Representatives; (b) provided to Recipient by a third-party contractor of Exelon, customer of Exelon or other Person designated by Exelon; or (c) sent by Recipient to a third-party contractor of Exelon, customer of Exelon or other Person designated by Exelon in connection with sharing Exelon's Confidential Information.

"Exelon Representatives" means Exelon Corporation and its affiliates, and/or any of their respective officers, employees, agents, contractors, consultants, insurers, attorneys, or representatives.

"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.

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

"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 Recipient's or Recipient Representatives' accessing, processing, storing or transmitting Exelon Electronic Confidential Information or Restricted Confidential Information.

"**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 Exelon or its Affiliates that would be considered important by a reasonable investor in deciding whether to buy, sell or hold securities of the Exelon 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 Exelon to deliver everything from simple cloud-based apps to sophisticated, cloud-enabled enterprise Applications.

"Person" means any natural person, partnership (limited, general, or other), joint venture (limited or otherwise), company (limited liability or otherwise), corporation, association, Governmental Authority, or any other legal entity of whatever kind or nature, together with any combination of one or more of the foregoing.

"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. §1029I; (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 Exelon 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.

"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 Exelon; (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; or (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 Recipient manages and provides to the Exelon 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 Exelon Electronic Information and Assets.

"Security Controls" mean safeguards or countermeasures to avoid, detect, counteract or minimize security risks to Exelon 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.

"**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) Exelon'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 licencee'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 Exelon 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.

ARTICLE 3 - RECIPIENT'S INFORMATION SECURITY PROGRAM

3.1 Recipient will document, implement, and maintain an Information Security Program to protect the integrity, availability, and confidentiality of Exelon's Electronic Confidential Information in accordance with the requirements set forth in this Exhibit 1.

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

3.3 Recipient will provide annual information security awareness refresher training to Recipient Representatives who have access to Exelon's Electronic Confidential Information, including the key elements of the Information Security Program and standards for the secure handling of Exelon's Electronic Confidential Information.

ARTICLE 4 - RECIPIENT'S ACCESS MANAGEMENT PROGRAM

4.1 Recipient will only grant access to Recipient's Electronic Information Assets where Exelon Electronic Confidential Information is processed, stored, or transmitted to Recipient Representatives who need access for the Purpose and will revoke such access promptly once the Person no longer requires or is no longer qualified for access.

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

4.3 Recipient will limit Administrator Account access to Exelon Electronic Confidential Information being processed, stored or transmitted using Recipient's Electronic Information Assets to only those Recipient Representatives whose job role and responsibilities require such access.

4.4 Recipient will ensure that Administrator Account ID passwords are changed immediately upon an assigned User's notification of termination or change in job role that no longer requires such access.

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

4.6 Recipient will immediately remove Recipient Representatives' access to any Exelon Electronic Confidential Information and Recipient Electronic Information Assets where Exelon Electronic Confidential Information is stored when: (i) the individual no longer requires access to a given Electronic information resource or Electronic Information Asset; (ii) the individual is terminated or his or her employment is otherwise ended, or (iii) when Recipient reasonably believes the individual may pose a threat to the safety or security of Exelon's Electronic Confidential Information.

4.7 Where the Recipient allows Recipient Representatives to use personal devices to access or transmit Exelon Electronic Confidential Information processed, stored, or transmitted in Recipient's Electronic Information Assets, the Recipient will implement Security Controls that are at least as restrictive as those provided in Exelon's Acceptable Use Policy and commensurate with the sensitivity of the Exelon Electronic Confidential Information.

ARTICLE 5 - RECIPIENT DATA BACKUP OF EXELON ELECTRONIC CONFIDENTIAL INFORMATION

5.1 Recipient will develop, implement, maintain, review and monitor a Data Backup Plan to protect the confidentiality, integrity, and availability of Exelon'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 - RECIPIENT'S USE OF CRYPTOGRAPHY

6.1 Recipient will utilize AES-256 bit or larger key size and will comply with password requirements in this Exhibit when an SSH Communications Security LLC Secure Shell cryptographic protocol is used.

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

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

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

7.2 Recipient'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 Recipient will immediately inform Exelon upon becoming aware of any Cyber Security Incident.

7.4 Recipient will immediately provide a verbal report of any Cyber Security Incidents to the Exelon Security Operations Center by telephone (to 1-800-550-6150, international at 410-470-5800), and follow up by email (to ESOC@exeloncorp.com and to maprequest@exelon.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. Recipient will provide written updates of the notice to Exelon 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 Exelon.

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

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

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

ARTICLE 8 - RECIPIENT'S SECURITY PATCH MANAGEMENT

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

ARTICLE 9 - RECIPIENT'S PASSWORD MANAGEMENT

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

9.2 Recipient will require all Recipient Representatives to comply with Recipient'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).

9.4 Recipient will ensure automatic logoff or locking is implemented and enforced, requiring all users to re-input their password 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.

ARTICLE 10 - RECIPIENT'S PHYSICAL SECURITY

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

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

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

10.4 Recipient will have processes and procedures for the control and monitoring of visitors' and other external persons' physical access to Recipient's Electronic Information Assets on which Exelon'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 - RECIPIENT'S MALWARE PROTECTION

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

11.2 Recipient 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

Recipient 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 Recipient's acts, errors, or omissions , including: (i) breaches of Exelon's information security Policies and Procedures, or the applicable security terms of this Agreement; (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; (vi) Internet advertising and content offenses; and (vii) defamation. Such insurance will address all of the foregoing, without limitation, when caused by Recipient or Recipient Representatives in accessing, processing, storing or transmitting Exelon Electronic Confidential Information. 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 Recipient will document, implement, and maintain a Business Continuity Plan to protect the privacy, confidentiality, integrity, and availability of Exelon's Electronic Information, Electronic Information Assets, and Digital Materials in the event of a disaster or interruption of Recipient's business.

13.2 The Business Continuity Plan will 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 Recipient Business Continuity Program will include back-up, disaster recovery and storage capabilities so as to protect the privacy, confidentiality, integrity, and availability of Exelon's Electronic Information, Electronic Information Assets. Recipient's responsibilities will include the following:

13.3.1 Recipient will back-up and store Exelon 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 Recipient will encrypt Exelon Data when being transmitted or stored outside of Exelon's computer systems and network. Exelon Data will be classified according to Exelon's required levels of classification.

13.3.3 Recipient 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 Purpose. Backed up data will be encrypted.

13.3.4 Recipient will develop, maintain and upon request, certify the implementation of a Business Continuity Plan to Exelon including plans, measures and arrangements, which permits Recipient to recover its facility, data, assets and personnel within reasonable timeframes.

13.3.4.1 In the event of a disaster, Recipient maintains responsibility for providing the services in accordance with the Business Continuity Plan.

13.3.4.2 Recipient will provide a report summary following each and any disaster or business interruption which should include measuring performance against the Business Continuity Plan and identification of problem areas and plans for resolution.

13.3.5 Recipient's Business Continuity Plan summary will be made available to Exelon upon request.

EXHIBIT 2 – ADVANCED CYBER AND INFORMATION SECURITY SPECIAL TERMS AND CONDITIONS

ARTICLE 1 - SCOPE

1.1 Article 3 (Recipient Cyber And Information Security Program Requirements) of this Exhibit 2 is applicable when Recipient or Recipient Representatives use their Electronic Information Assets to: (1) access, process, store or transmit Exelon Electronic Restricted Confidential Information (2) provide Digital Materials for installation on or connection to Exelon's Electronic Information Assets; (3) perform Digital Services on either Exelon's Electronic Information Assets or Digital Materials that will be installed on or connected to Exelon's Electronic Information Assets; or (4) provide Cloud Computing Services to Exelon which access, process, store or transmit Exelon's Electronic Restricted Confidential Information.

1.2 Article 4 (Recipient's Remote Access To Exelon Electronic Information Assets) of this Exhibit 2 is applicable when Recipient or Recipient Representatives will access Exelon Electronic Information Assets from Recipient Electronic Information Assets using Remote Access Systems.

1.3 Article 5 (Digital Materials and Services Security Requirements) of this Exhibit 2 is applicable when Recipient or Recipient Representatives provide Digital Materials for installation on or connection to Exelon's Electronic Information Assets or perform Digital Services on Exelon's Electronic Information Assets or Digital Materials that will be installed on or connected to the Exelon's Electronic Information Assets.

1.4 Article 6 (Cloud Computing Services Security Requirements) of this Exhibit 2 is applicable when Recipient or Recipient Representatives provide Cloud Computing Services to Exelon which access, process, store or transmit Exelon's Electronic Restricted Confidential Information.

1.5 Article 7 (Direct Network Connection Security Requirements) of this Exhibit 2 is applicable when Recipient or Recipient Representatives have a Direct Network Connection to Exelon's Electronic Information Assets.

1.6 Article 8 (Off-Shore Locations Security Requirements) of this Exhibit 2 is applicable where Recipient or Recipient Representatives will operate from an Off-Shore Location and: (1) require or engage in accessing, processing, storing or transmitting of Exelon's Electronic Restricted Confidential Information; or (2) access Exelon Electronic Information Assets from Recipient Electronic Information Assets using Remote Access Systems; (3) provide Digital Materials for installation on or connection to Exelon's Electronic Information Assets; (4) perform Digital Services on either Exelon's Electronic Information Assets or Digital Materials that will be installed on or connected to the Exelon's Electronic Information Assets; (5) provide Cloud Computing Services to Exelon which access, process, store or transmit Exelon's Electronic Restricted Confidential Information; or (6) have a Direct Network Connection to Exelon's Electronic Information Assets.

1.7 Article 9 (Use of Transient Cyber Assets and Removable Media) of this Exhibit 2 is applicable where Recipient or Recipient Representatives need to connect their Removable Media or Transient Cyber Asset to any Exelon BES Cyber System;

1.8 Article 10 (Cyber and Information Security Audit) and Article 11 (Cyber Security Incident/Network Security Insurance) of this Exhibit 2 is applicable when any of Articles 2-9 are applicable.

ARTICLE 2 - DEFINITIONS

Capitalized terms not defined herein will have the meaning given to them elsewhere in the Agreement, including in Exhibit 1 (Basic Cyber and Information Security Special Terms and Conditions).

"**Access Level"** means a position in a hierarchy of access rights to an Electronic Information Asset that determines what actions a User is authorized to take on that Asset.

"**Ad-Hoc Mode**" means a method for wireless computer networks, WLAN network or other Wireless Devices to directly communicate with each other without the use of an AP. Ad-Hoc Mode may also be referred to as a peer-to-peer mode.

"**AES"** means Advanced Encryption Standard and is an encryption algorithm specification for the encryption of electronic data established by the National Institute of Standards and Technology.

"**AP**" means access point.

"**Build Procedure**" means a step-by-step procedure that describes how to configure or set up a particular Application, platform, or system.

"**BYOD"** means "Bring Your Own Device" and refers to Wireless Devices not issued by Recipient but permitted to be used by Recipient to access Recipient's WLAN.

"Certificate Authority" means an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate.

"**CISS**" means the Corporate and Information Security Services division of Exelon Business Services Company.

"Cloud Controls Matrix" means a baseline set of Security Controls created by the Cloud Security Alliance to help enterprises assess the risk associated with a cloud computing provider.

"CSRM" or **"Cloud Security Requirements Matrix"** means a Exelon security questionnaire that reviews the Security Controls of a Cloud Computing Service that Exelon plans to utilize to fulfill a business need.

"Cloud Security Alliance" is an organization which defines and raises awareness of best practices to help ensure a secure cloud computing environment (https://cloudsecurityalliance.org).

"COBIT" means Control Objectives for Information and Related Technologies which is a framework created by ISACA for information technology (IT) management and IT governance

"Credentials" means the properties of a process that are used for determining access rights.

"Critical Vulnerabilities" means Vulnerabilities that must be patched outside of normal patching cycles because of an increased risk or active exploitation.

"Cyber Attack" means an attempt by hackers to damage or destroy a computer network or system, including denial of service attacks, phishing and social engineering.

"**Data Leakage**" means unauthorized transmission of data from within an organization to an external destination or recipient.

"**Deployment Plan**" has the meaning given in Section 8.2.5.1.

"**Direct Network Connection**" means a dedicated network connection between Recipient and Exelon's network.

"**DSA**" means Digital Security Algorithm.

"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).

"**End-of-Life Operating Systems**" means digital operating systems for which the Recipient or third-party supplier (e.g. developer, licensor or owner) no longer provides automatic fixes, updates, Security Patches or online technical assistance and support.

"Exelon's Designated Representative" means the individual or individuals designated by Exelon who will provide the general administration of the Agreement in connection with this Agreement. Exelon may, in its sole discretion, change its representatives at any time or from time to time, and will promptly notify Recipient, in writing, of any such change.

"**FIPS 140-2 Level 2**" means Federal Information Processing Standard Publication 140-2, Level 2, a U.S. Government computer security standard used to accredit cryptographic modules. Level 2 improves upon the physical security mechanisms of a Security Level 1 cryptographic module by requiring features that show evidence of tampering, including tamper-evident coatings or seals that must be broken to attain physical access to the plaintext cryptographic keys and critical security parameters (CSPs) within the module, or pick-resistant locks on covers or doors to protect against unauthorized physical access.

"Firewall" means a network security system designed to monitor and control incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.

"Guest Wireless Access" means a dedicated wireless network that is virtually segregated from the corporate WLAN. It usually uses the same infrastructure as the corporate WLAN but is virtually segregated or zoned off.

"IDS/IDP" means Intrusion Detection System / Intrusion Prevention System.

"IASME Governance" means Information Assurance for Small and Medium Enterprises Consortium.

"**Infrastructure Syslog Information**" means messages sent from a variety of devices reporting different events and collected on a single logging server—the syslog server.

"ISACA" means Information Systems Audit and Control Association, an international professional association focused on IT governance.

"ISO/IEC 27000 Series Information Security Standards" means a series of best practices published by ISO (the International Organization for Standardization) and the IEC (International Electrotechnical Commission) to help organizations improve their information security.

"ISO 27001/27002" means the international standards that sets out the specification for an information security management system (ISMS). Its best-practice approach helps organizations manage their information security by addressing people and processes as well as technology.

"ISO 27005" means the international standard that describes how to conduct an information security risk assessment in accordance with the requirements of ISO 27001.

"**MFA"** means multi-factor authentication method of computer access control in which a User is only granted access after successfully presenting several separate pieces of evidence to an authentication mechanism (e.g., passwords, PINs, etc.).

"NIST" means National Institute of Standards and Technology

"NIST SP 800" means the NIST set of documents that describe United States Federal Government computer security policies, procedures and guidelines.

"NIST SP 800-53" means the NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organization which includes a set of standards and guidelines to help federal agencies and contractors meet the requirements set by the Federal Information Security Management Act (FISMA).

"NIST Cybersecurity Framework" means the NIST policy framework of computer security guidance for how organizations can assess and improve their ability to prevent, detect, and respond to Cyber Attacks.

"Off-Shore Location" means any location outside of the fifty United States and the District of Columbia.

"Out-of-Band Management" means the use of a dedicated channel for managing network devices. This allows the network operator to establish trust boundaries in accessing the management function top apply it to network resources.

"**OWASP ASVS**" means the most current version of the Open Web Application Security Project Application Security Verification Standard found at https://www.owasp.org.

"PCA" or **"Protected Cyber Asset"** means one or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter (as defined by NERC). The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.

"Penetration Testing" means an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system and identify strengths and weaknesses.

"Pre-Shared Key" means a shared secret key which was previously shared between two parties using a secure channel before it needs to be used.

"**Principle of Least Privilege"** means that in a particular abstraction layer of a computing environment, every module (such as a process, a User, or a program, depending on the subject) must be able to access only the information and resources that are necessary for its legitimate purpose. For example, Users must only be granted access to Exelon Electronic Information or Exelon Electronic Information Assets on a need-to-know basis and to the extent such access is required for his/her assigned job function.

"Public Network Segment" means network components that are not owned, operated, or managed solely by Exelon.

"**RBAC**" means Role-Based Access Control.

"**Removable Media"** means portable or removable hard disks, floppy disks, USB memory drives, zip disks, optical disks, CDs, DVDs, digital film, memory cards (e.g., Secure Digital (SD), Memory Sticks (MS), CompactFlash (CF), SmartMedia (SM), MultiMediaCard (MMC), and xD-Picture Card (xD)), magnetic tape, and all other removable data storage media

"Secure System Development Lifecycle " means the security requirements and tasks that must be considered and addressed within systems, projects or Applications that are created or updated to address a business need, including the Common Criteria, Microsoft Security Development Lifecycle, NIST 800-61 Volume 1, the OWASP ASVS, the OWASP Comprehensive, Lightweight Application Security Process, ISA 62443-4-1, or the UL 2900 Outlines.

"**Security Event Monitoring System**" means a system for holistic monitoring of an organization's Security Controls.

"Security Gateway" means a security solution that prevents unsecured traffic from entering an internal network of an organization.

"SRA" or **"Security Risk Assessment"** means a questionnaire comprised of Exelon's Security Controls provided and completed by the Recipient to ensure Recipient meets Exelon's Security Control requirements.

"Security Risk and Threat Management Program" means a program designed to identify, assess, and control threats to an organization's Electronic Information and Electronic Information Assets.

"SHA" means Secure Hash Algorithm.

"SIEM" means Security Information and Event Management.

"SOC Report Type 2" means the American Institute of Certified Public Accountants ("AICPA") Service Organization Control Type 2 report on management's description of a service organization's system and the suitability of the design and operating effectiveness of controls under the AICPA's Trust Services Principles and Criteria of Security, Availability, Processing Integrity, Confidentiality, or Privacy and the AICPA's Standards for Attestation Engagements (SSAE) 16 Type II.

"**Standard Build Image**" means a copy of complete and functioning computer system that can be simply copied to a new system.

"**Standard Configuration**" means specific asset configuration parameters approved by Exelon .

"Standard Configuration Documents" means the documentation that defines the specific asset configuration parameters approved by Exelon.

"Summary Documentation on Vulnerabilities" has the meaning in Section 5.6.1 of this Exhibit 2.

"TCA" or "Transient Cyber Asset," as defined by NERC, mean a Cyber Asset that (i) is capable of transmitting or transferring executable code, (ii) is not included in a BES Cyber System, (iii) is not a PCA, and (iv) is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless, including near field or Bluetooth communication) for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an Electronic Security Perimeter, or a PCA. Examples include, but are not limited to, Cyber Assets used for data transfer, Vulnerability assessment, maintenance, or troubleshooting purposes.

"**TLS 1.2"** means Transport Layer Security 1.2, a cryptographic protocol defined in Request for Comment (RFC) 5246 (August 2008) that provides communications security over a computer network.

"Vulnerability Scans" means a process to assess Applications, System Software, computers, and networks and other Electronic Information Assets to identify and detect Vulnerabilities arising from misconfigurations or flawed programming with assets such as a firewall, router, web server, or application server.

"**Wireless Device"** means any type of device that communicates with other devices without needing a physical connection to the other device to transfer and receive information.

"**WPA2 Standard Requirements"** means the Wi-Fi Protected Access 2 security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks.

"**WLAN"** means Recipient's Wireless Local Area Network over which Exelon's Electronic Information may be stored or transmitted.

ARTICLE 3 - RECIPIENT CYBER AND INFORMATION SECURITY PROGRAM REQUIREMENTS

3.1 Applicability

This Article 3 is applicable when Recipient or Recipient Representatives access, process, store or transmit Exelon Electronic Restricted Confidential Information using Recipient or Recipient Representatives' Electronic Information Assets.

3.2 Recipient's Information Security Program

In addition to the requirements in Article 3 (Recipient's Information Security Program) of Exhibit 1 (Basic Cyber and Information Security Special Terms and Conditions), the Recipient Information Security Program will adopt, or be certified by one or more of: (i) Cloud Security Alliance STAR Certification; (ii) COBIT; (iii) IASME Governance; (iv) ISO/IEC 27000 Series Information Security Standards;) (v) NIST SP 800-53; (vi) NIST Cybersecurity Framework; (vii) SOC Reports Type 2; or (viii) other Exelon-approved standards or certifications.

3.3 Recipient's Access Management Program

In addition to the requirements of Article 4 (Recipient's Access Management Program) in Exhibit 1 (Basic Cyber and Information Security Special Terms and Conditions):

3.3.1 Access Control

3.3.1.1 Recipient will use RBAC to approve and authorize Recipient Representatives access to either Contractor's Electronic Information Assets.

3.3.1.2 Contractor will install security warning banners on Recipient Electronic Information Assets including language to the effect that access and use of such assets and information is only by authorized individuals, access is monitored, and unauthorized or illegal use will be prosecuted.

3.3.2 Access Requests and Approvals

3.3.2.1 Recipient will ensure all requests for access to Exelon Electronic Restricted Confidential Information accessed, processed, stored or transmitted using Recipient's Electronic Information Assets are reviewed and approved by a Recipient manager before Recipient's authorized administrators grant access.

3.3.2.2 Recipient will document Recipient Representatives who have access to Exelon's Electronic Restricted Confidential Information accessed, processed, stored or transmitted using Recipient's Electronic Information Assets. Documentation will include the Recipient Representatives' Access Levels and the Recipient manager who approved their access. Upon request, Recipient will provide that documentation to Exelon.

3.3.2.3 Recipient will review the list(s) of authorized approvers periodically, preferably every 90 days or at least annually.

3.3.2.4 Recipient will maintain and make available upon Exelon's request a record of all Recipient Representatives requests for access to Exelon Electronic Restricted Confidential Information accessed, processed, stored or transmitted using Recipient's Electronic Information Assets for a minimum of two (2) years from the date of such request, with the following information included for each request: (i) date of access request; (ii) requestor name; (iii) User (requested for) name; (iv) system and/or Application name; (v) Access Level requested for the system and/or Application; (vi) need for access; (vii) approver name(s); (viii) date of approval(s); (ix) date access was provisioned; (x) Date of access removal request; (xi) date access was removed; and (xii) reason for removal of access.

3.3.3 Authentication

3.3.3.1 Recipient Representatives will not write down authentication credentials, such as User Account IDs and passwords, or store them in readable form in automatic login scripts, software macros, terminal function keys, in computers without access control, shortcuts, and/or in other locations where unauthorized persons might discover them.

3.3.3.2 Recipient will protect authentication information (e.g. user name, password, or other authentication information) while it is Data-At-Rest and Data-In-Transit with NIST-approved cryptographic standards and algorithms as documented in NIST SP 800-175a and NIST SP 800-175b to prevent unauthorized individuals from obtaining the data.

3.3.4. Administrator Accounts

Where technically feasible, Recipient will log and monitor all activity of Recipient Representatives with Administrative or Shared Account IDs while they are accessing Exelon Electronic Restricted Confidential Information being processed, stored or transmitted using Recipient's Electronic Information Assets.

3.3.5 Access Reviews

3.3.5.1 Recipient will review and verify Recipient Representatives5' continued need for access to Exelon Electronic Restricted Confidential Information processed, stored or transmitted using Recipient's Electronic Information Assets and Access Level on an annual basis.

3.3.5.2 Recipient will retain evidence of the reviews for two years from date of each review.

3.3.6 Password Requirements

3.3.6.1 If biometric controls are used in lieu of, or in addition to, passwords, the biometric methods will be disclosed to Exelon's Designated Representative.

3.3.6.2. Recipient will ensure that passwords are not displayed on any screens or reports.

3.3.6.3. Recipient will ensure passwords are delivered via a secure and reliable method; which could include confirming emails to the account holder that do not contain the account name, and a secure temporary password which is changed immediately upon login.

3.3.7 Session Management

3.3.7.1. Recipient Applications and Recipient Electronic Information Assets with access to Exelon Electronic Restricted Confidential Information using Recipient's Electronic Information Assets, will automatically disconnect after no more than thirty (30) minutes of inactivity during a session.

3.3.7.2 The Account ID will be disabled after a reasonable threshold is met for the number of invalid login attempts.

3.3.7.3 Once an Account ID has been disabled due to reaching the maximum number of invalid login attempts, the Account ID may be automatically reset after a reasonable period (no less than 15 minutes) for systems that support an account reset feature.

3.4 Recipient's Secure Asset Lifecycle Program

3.4.1 Recipient's Asset Management Program will include the development, implementation, maintenance, review and monitoring of ownership, inventory, return, and acceptable uses of Recipient Electronic Information Assets.

3.4.2 Recipient will ensure accurate and timely inventory of Recipient Electronic Information Assets that access, process, store, or transmit Exelon's Electronic Restricted Confidential Information.

3.4.3 Recipient will review its Electronic Information Asset inventory annually to validate that it is current, complete, and accurate.

3.4.4 Recipient will permanently delete or securely overwrite all Exelon Restricted Confidential Information on Recipient Electronic Information Assets prior to their transfer to a third-party or disposal.

3.5 Recipient's Data Leakage Prevention

3.5.1 In addition to the requirements of Article 5 (Recipient Data Backup of Exelon Electronic Confidential Information) in Exhibit 1 (Basic Cyber and Information Security Special Terms and Conditions), Recipient will have a program to prevent Data Leakage, including email, internet/web gateway, USB, optical and other forms of ports/portable storage, mobile computing and BYOD, Remote Access Systems, and file sharing mechanism.

3.5.2 Recipient will not connect Removable Media or Transient Cyber Asset to any Exelon BES Cyber System.

3.6 Recipient's Use of Cryptography

In addition to the requirements of Article 6 (Recipient's use of Cryptography) in Exhibit 1 (Basic Cyber and Information Security Special Terms and Conditions):

3.6.1 Recipient will use NIST-approved cryptographic standards and algorithms as documented in NIST SP 800-175b with sufficient key lengths for encryption, integrity checking, and authentication of origin of Exelon Electronic Information.

3.6.2 When an RSA Security LLC (**"RSA"**) cryptographic network protocol is used, the required minimum key length is 2048 bits (4096 bits is preferred).

3.6.3 When an SSH Communications Security, LLC Secure Shell (**"SSH"**) cryptographic network protocol is used, Recipient will utilize AES-256 bit or larger key size and will comply with password requirements in this Exhibit.

3.6.4 Recipient's cryptographic infrastructures will provide all necessary primitives, functions, and operations to support any future upgrade to FIPS 140-2 Level 2 compliance.

3.6.5 Recipient will use TLS 1.2 or higher with bi-directional authentication to secure the transmission of Exelon's Restricted Confidential Information.

3.6.6 Recipient will use cryptographic standards and algorithms to secure Exelon Restricted Confidential Information that are: (i) public domain, including source code, (ii) are peer reviewed and approved by NIST, and (iii) will not be known to have been compromised in practice.

3.6.7 Recipient will use algorithms to secure Exelon Restricted Confidential Information that are: (i) public domain, including source code, (ii) are peer reviewed and approved by NIST, and (iii) will not be known to have been compromised in practice.

3.6.8 Recipient will encrypt internal communication between Application components, peer hosts, databases, and middleware where technically feasible.

3.6.9 Recipient's encryption controls will be free from known defect and patched within 30 days upon identification of a Vulnerability.

3.7 Recipient's Logging and Monitoring Processes

3.7.1 Recipient will document, implement, and maintain logging and monitoring process which ensures that key systems are set to log key events with such logs being retained for a minimum period of twelve (12) months.

3.7.2 The logs should contain events including, start and stop points of the logged process, changes to the type of logged events, system start-up and shut-down, successful logins, failed login attempts, and creation, modification and deletion to/of user accounts for all Recipient Representatives s who have access to Exelon's Electronic Restricted Confidential Information from locations where the computer and network facilities are not under the control of the Exelon.

3.7.3 Key logging events will be reviewed on at least a monthly basis to detect for any unauthorized activities and targets of a Cyber Attack.

3.8 Recipient's Network Security

3.8.1 Recipient will use network security infrastructure, including Firewalls, IDS/IPS, anti-phishing software and other Security Controls, that provide continuous monitoring, have the capability to restrict unauthorized network traffic, and detect and limit the impact of Cyber Attacks.

3.8.2 Network traffic will be appropriately segregated with routing and access controls separating traffic on internal networks from public or other untrusted networks, where technically feasible.

3.8.3 Recipient will scan its externally facing and internal Electronic Information Assets with applicable industry standard security vulnerability scanning software to uncover Vulnerabilities, ensure that such systems and other resources are properly hardened, and identify any unauthorized wireless networks.

3.8.4 Recipient will maintain a formal process for approving, testing, and documenting all network connections and changes to its Firewall and router configurations.

3.8.5 Recipient will configure Firewalls to deny and log suspicious packets and restrict to only allow appropriate and authorized traffic, denying all other traffic through the firewall.

3.8.6 Recipient will review and, if necessary, update Firewall configurations every six (6) months.

3.8.7 Recipient will leverage network specific information Security Controls to protect Exelon's Electronic Restricted Confidential Information that are accessed by, stored on, processed by, or transmitted over Recipient's Electronic Information Assets.

3.8.8 Recipient will employ, securely configure, and regularly update and test enterprise-wide Firewall infrastructure to restrict access to and from untrusted networks and minimize access to extent needed to perform services.

3.8.9 Recipient will use secure protocols to protect transmission of Exelon's Electronic Restricted Confidential Information and Credentials (examples of unacceptable protocols are FTP, telnet, and early implementations of SSL/TLS 1.1 or below).

3.9 Recipient's Security Patch Management

In addition to the requirements of Article 8 (Recipient's Security Patch Management) in Exhibit 1 (Basic Cyber and Information Security Special Terms and Conditions):

3.9.1 Recipient will promptly assess Vulnerabilities and identify and deploy all applicable Security Patches for each Recipient Electronic Information Asset (e.g., Applications, System Software, and components including drivers, subsystems, programming languages, libraries and BIOS).

3.9.2 Recipient will deploy all Security Patches promptly, in accordance with the criticality of an identified Vulnerability.

3.9.3 Recipient will provide a Security Patch or other corrective action as soon as possible, but in no event later than sixty (60) days from the notification to Exelon of such Vulnerability.

3.9.4 Recipient will have a process in place to reassess Vulnerabilities to determine whether the Security Patch closed the Vulnerability.

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

3.10 Recipient's Cyber Security Risk And Threat Management

3.10.1 Cyber Security Risk Management Program

3.10.1.1 Recipient will document, implement, and maintain a Security Risk and Threat Management Program in place that identifies and mitigates risks associated with and threats to the Recipient's Electronic Information Assets on which Exelon's Electronic Restricted Confidential Information is stored, in accordance with current standards (e.g., NIST SP 800, ISACA COBIT, ISO 27005, etc.).

3.10.1.2 Recipient's Security Risk and Threat Management Program will include assessing Vulnerabilities in Recipient's Electronic Information Assets, identifying internal and external threats to Recipient's Electronic Information Assets, assessing potential impacts to Exelon's Electronic Restricted Confidential Information.

3.10.1.3 Recipient's Security Risk and Threat Management Program policies and procedures will be made available upon Exelon's reasonable request.

3.10.2 Security Risk Assessment

3.10.2.1 Recipient will conduct an annual cyber and physical security risk assessment to evaluate and monitor its exposure to information security risks and threats on an annual basis.

3.10.2.2 Recipient will ensure that any risks and threats identified as part of the cyber and physical security risk assessment are prioritized and appropriate actions are taken to address those risks and threats.

3.10.2.3 Recipient will notify Exelon if any risks or threats cannot be remediated.

3.10.2.4 Recipient will provide a written report of the results of the annual cyber and physical security risk assessment to Exelon upon request.

3.10.3 Cyber Security Forms and Questionnaires

3.10.3.1 Recipient will complete Exelon's cybersecurity forms and questionnaires (e.g., SRA or CSRM) prior to beginning to access, process, store or transmit Exelon Electronic Restricted Confidential Information for Exelon and will update these cybersecurity forms and questionnaires going forward at such times as are determined by Exelon.

3.10.3.2 Recipient warrants the completeness and accuracy of its responses on these cybersecurity forms and questionnaires at the time they are submitted.

3.10.3.3 Recipient will resolve security findings resulting from Exelon's review of the cybersecurity forms and questionnaires.

3.10.4 Cyber Security Threat Assessment Participation

Recipient will participate with Exelon in an annual tabletop exercise of cyber and/or physical security threats if requested by Exelon.

3.11 Recipient's Vulnerability Management Processes

3.11.1 Recipient will document, implement, and maintain Vulnerability management processes to designed to eliminate Vulnerabilities that could be exploited by malware or other methods.

3.11.2 Recipient Vulnerability management processes should include Vulnerability identification, communication, remediation, Security Patching and hardware maintenance.

3.11.3 Recipient will ensure there are processes established to receive, analyze and respond to Vulnerabilities disclosed to the organization from internal and external sources.

3.11.4 Recipient will ensure identified Vulnerabilities are mitigated or documented as accepted risks.

3.11.5 Recipient will document and manage Vulnerability scanning findings and remediate issues within a reasonable timeframe.

3.11.6 Recipient will upon reasonable request permit Exelon access to Penetration Testing reports relevant to the services being provided.

3.12 Recipient's Wireless Security

3.12.1 Where technically feasible, Recipient will enable, configure, and monitor embedded intrusion detection protection functions within its WLAN infrastructure.

3.12.2 Where technically feasible, Recipient's and Recipient Representatives' WLAN Infrastructure Syslog Information will be forwarded to a Security Event Monitoring System and monitored for Cyber Security Incidents.

3.12.3 Recipient will have policies, procedures, and practices implemented for governing Wireless Devices accessing Recipient's WLAN, and have a process in place to ensure that the Security Controls are not bypassed, including Ad-Hoc Mode, Rogue AP devices, etc.

3.12.4 Recipient will allow only Recipient-approved Wireless Devices to connect to Recipient's WLAN, except as provided in Section 2.14.8 (BYOD WLAN Access).

3.12.5 WLAN Configuration Requirements

3.12.5.1 Recipient will use WLAN network encryption standards which meet or exceed 128-bit AES encryption and conform to the key lengths specified in Section 2.5.1 of this Exhibit 2.

3.12.5.2 Recipient will set its WLAN authentication for 802.1x and EAP- TLS.

3.12.5.3 The Pre-Shared Key for WPA2 Standard Requirements wireless access to Recipient's WLAN will be a minimum of 20 characters in length and randomly generated.

3.12.6 User Configuration Requirements

3.12.6.1 Recipient will ensure that all Wireless Devices or systems connecting with Recipient's WLAN comply with WPA2 Standard Requirements or higher.

3.12.6.2 Recipient will use digital certificates issued by an approved digital certificate management utility (e.g., CISCO ISE, Radius, etc.) to establish the connection between supplicant (client) and the management server on Recipient's WLAN.

3.12.6.3 Recipient will install a digital certificate from a commercial or Recipient self-signed Certificate Authority on the digital certificate management server as the "trusted" root certificate for the WLAN clients.

3.12.6.4 This trusted root certificate will be distributed as part of Recipient's standard desktop image so that all Recipient-approved desktops are capable of communicating over secure channels.

3.12.7 Guest Wireless Access

3.12.7.1 Network traffic for Guest Wireless Access will be segregated from Recipient WLAN traffic, routed solely to the Internet, and logged and filtered by content filters.

3.12.7.2 Recipient-issued Wireless Devices and Exelon's Electronic Information Assets will not be configured for Guest Wireless Access.

3.12.8 BYOD WLAN Access

3.12.8.1 Recipient will segregate WLAN traffic for BYODs from both its WLAN traffic for Recipient-issued Wireless Devices and its Guest Wireless Access.

3.12.8.2 Recipient will limit BYOD access to Applications and Systems Software on which Exelon's Electronic Information is transmitted or stored to only Users who have been approved and authorized by Recipient.

3.12.8.3 Recipient will log and filter BYOD network traffic using content filters to monitor user and device resource access.

3.12.8.4 Recipient will ensure that BYOD authentication adheres to and enables the WPA2 Standard Requirements or higher for personal wireless access.

3.12.8.5 Recipient-issued Wireless Devices will not be configured to connect to Recipient's BYOD WLAN.

3.12.9 Monitoring and Management

3.12.9.1 Recipient will document and maintain Standard Configuration settings for Recipient's WLAN infrastructure.

3.13.9.2 Recipient will implement rogue AP detection capabilities and will disable/disconnect the rogue APs.

ARTICLE 4 - RECIPIENT'S REMOTE ACCESS TO EXELON ELECTRONIC INFORMATION ASSETS

4.1 Applicability

This Article 4 is applicable when Recipient or Recipient Representatives will access Exelon Electronic Information Assets from Recipient Electronic Information Assets using Remote Access Systems.

4.2 Access Control

4.2.1 Exelon will individually review and approve Recipient Representatives requests for access to Exelon's Electronic Information Assets using Remote Access Systems.

4.2.2 Recipient Representatives will not remotely access Exelon's Electronic Information Assets from public wireless networks, including cafes, restaurants, hotels, airports, etc.

4.2.3 Recipient Representatives will use MFA in combination with encryption to establish a remote connection to Recipient's Electronic Information Assets.

4.2.4 Recipient Representatives using wireless connections to remotely access Exelon's Electronic Information Assets Recipient will use encryption standards which meet or exceed NIST-approved cryptographic standards and algorithms as documented in NIST SP 800-175b.

4.3 Authentication

4.3.1 Recipient will prohibit Recipient Representatives from saving their remote access and MFA credentials to Exelon Electronic Information Assets through automatic login scripts, software macros, terminal function keys, or use of autosave.

4.3.2 Recipient Representatives will not share their Remote Access Systems credentials (e.g., User ID, passwords, and PINs) with anyone.

4.4 Acceptable Use

Recipient and Recipient Representatives will comply with Exelon's Acceptable Use Policy (SY-AC-6) when using Remote Access Systems to access Exelon's Electronic Information Assets.

ARTICLE 5 - DIGITAL MATERIALS AND SERVICES SECURITY REQUIREMENTS

[NOT USED]

ARTICLE 6 - CLOUD COMPUTING SERVICES SECURITY REQUIREMENTS

[NOT USED]

ARTICLE 7 - DIRECT NETWORK CONNECTION SECURITY REQUIREMENTS

7.1 Applicability

This Article 7 is applicable when Recipient or Recipient Representatives have a Direct Network Connection to Exelon's Electronic Information Assets.

7.2 Access Control

7.2.1 Recipient will permit Exelon to gather information relating to access, including Recipient's access, to Exelon's Electronic Information Assets. This information may be collected, retained and analyzed by Exelon to identify potential Vulnerability. This information may include from trace files, statistics, network addresses, and the actual data or screens accessed or transferred.

7.2.2 Recipient will immediately terminate any Direct Network Connection to Exelon's Electronic Information Assets if Recipient suspects there has been a breach of or unauthorized access to either Recipient's or Exelon's Electronic Information Assets, or upon Exelon's written instructions.

7.3 Logging And Monitoring

If the Direct Network Connection requires that Recipient implement a Security Gateway, Recipient will maintain logs of all sessions using such Security Gateway. These session logs will include sufficiently detailed information to identify the end user or Application, origination IP address, destination IP address, ports/service protocols used and duration of access. These session logs will be retained for a minimum of six (6) months from session creation.

7.4 Network Security

7.4.1 Recipient will implement a Firewall between Recipient's other Electronic Information Assets and Recipient Electronic Information Asset(s) with the Direct Network Connection to Exelon's Electronic Information Asset(s).

7.4.2 The Firewall will be configured to allow only the connections authorized by Exelon.

7.4.3 Recipient will not permit a physical or logical connectivity between other Recipient Electronic Information Assets and a Recipient Electronic Information Asset with a Direct Connection to Exelon's Electronic Information Asset.

7.4.4 Recipient will place Electronic Information Assets requiring a Direct Network Connection in a Public Network Segment to protect internal network resources.

7.4.5 Recipient will comply with all Exelon requirements for Direct Network Connections between Recipient Electronic Information Assets and Exelon's Electronic Information Assets.

7.4.6 Recipient will incorporate Exelon-approved cryptographic Security Controls for all inbound and outbound Direct Network Connections to Exelon's Electronic Information Assets.

ARTICLE 8 - OFF-SHORE LOCATIONS SECURITY REQUIREMENTS

8.1 Applicability

This Article 8 is applicable where Recipient or Recipient Representatives will access, process, store or transmit Exelon's Electronic Restricted Confidential Information to or from an Off-Shore Location.

8.2 Use of Off-Shore Locations

8.2.1 Recipient will not use an Off-Shore Location to access, process, store or transmit Exelon's Electronic Restricted Confidential Information without the prior express written approval of Exelon.

8.2.2. Contractor will not relocate or subcontract the performance of the Work from the United States to an Off-Shore Location, or from one Off-Shore Location to another Off-Shore Location, without the prior express written approval of Exelon.

8.3 Remote Access

In addition to the requirements of Article 4 (Remote Access to Exelon's Electronic Information Assets) of this Exhibit 2:

8.3.1 Recipient will use Exelon-approved Remote Access Systems and will route traffic from the Off-Shore Location through a Recipient office located in the United States.

8.3.2 Recipient will equip all Recipient Electronic Information Assets used to remotely connect to Exelon's Electronic Information Assets from Off-Shore Locations with the capability to report the Remote Access System's security baseline and installed software inventory using a Exelon-approved extract tool.

8.4 Extraction Or Exfiltration Of Data

8.4.1 Recipient will not permit extraction or exfiltration of Exelon's Electronic Restricted Confidential Information from Exelon's Electronic Information Assets onto the Recipient's, Recipient Representatives' or any third party's Electronic Information Assets in an Off-Shore Location.

8.4.2 Recipient will put Security Controls in place to detect and prevent data extraction and exfiltration from Exelon's Electronic Information Assets onto the Recipient's, Recipient Representatives' or any third party's Electronic Information Assets in an Off-Shore Location.

8.5 Minimum Configurations For Off-Shore Workspaces And Workstations

8.5.1 Recipient shall maintain physical access controls at approved Off-Shore Locations.

8.5.2 Recipient will configure all its Electronic Information Assets at its Off-Shore Locations used to access, process, store or transmit Exelon's Electronic Restricted Confidential Information to remove or disable screenshot, printer, and removable storage capabilities and/or software (e.g., SnagIt, Snipping Tool, Printers, USB, and DVD).

8.5.3 Recipient will not allow visual recording devices, including mobile phones and cameras into any Off-Shore Location workspaces where Exelon's Electronic Confidential Information is accessed, processed, stored or transmitted.

8.6 Information Security Personnel

Recipient will have competent information security personnel and Cyber Security Incident response teams whose job responsibilities include Cyber Security Incident response at its Off-Shore resource locations.

8.7 Initial And Annual Training Requirements

8.7.1 Recipient will conduct initial and annual refresher training and awareness programs at its Off-Shore Locations for Recipient Representatives who access, process, store or transmit Exelon's Electronic Restricted Confidential Information covering compliance with the confidentiality, cyber and information security, and privacy requirements of Exhibit 1 (Basic Cyber and Information Security Special Terms and Conditions, and Exhibit 2 (Advanced Cyber and Information Security Special Terms and Conditions).

8.7.2 Recipient will provide, and document, routine training to Recipient's information security personnel at its Off-Shore Locations on:

8.7.2.1 configuration and use of installed Data Loss Prevention tools for the Proper detection of data exfiltration.

8.7.2.2 use (configuration and monitoring) of the installed SIEM protocols and systems for the detection of Cyber Security Incidents.

8.7.2.3 use (tuning and monitoring) of installed IDS/IPS for the detection of malicious traffic.

8.7.2.4 use of (configuration, signature updates, testing) of the installed anti-Malware tools.

8.7.2.5 responding to a detected Cyber Security Incident or other security incident, including timely communications to Exelon, mitigating actions, and data preservation procedures.

8.7.3 Recipient's annual report in Section 8.8 (Compliance Self-Audits) will detail the training provided and listing all the Recipient Representatives who participated in the training and the dates of their participation.

8.8 Compliance Self-Audits

Recipient will perform an annual audit on Recipient's and its Recipient Representatives' compliance with the requirements of this Exhibit 2 at its Off-Shore Locations and provide the results to Exelon by upon request.

ARTICLE 9 - USE OF TRANSIENT CYBER ASSETS (TCAS) AND REMOVABLE MEDIA

[NOT USED]

ARTICLE 10 - CYBER AND INFORMATION SECURITY AUDITS

Exelon or its third-party designee may perform audits and security tests of Recipient's IT or systems environment to determine Recipient's compliance with this Exhibit 2. These audits and tests may include coordinated Penetration Testing and Vulnerability Scans, interviews of Recipient Representatives, review of documentation, and technical inspection of systems and networks as they relate to the receipt, maintenance, use, retention, and authorized destruction of Restricted Confidential Information. If Exelon desires to conduct unannounced Penetration Testing, Exelon will provide contemporaneous notice to Recipient's Vice President of Audit, or equivalent position. Recipient will provide all information reasonably requested by Exelon in connection with any such audits and will provide reasonable access and assistance to Exelon upon request. Recipient will comply with all reasonable recommendations that result from such inspections, tests, and audits within reasonable timeframes and at its own cost and expense. Exelon reserves the right to view, upon request, any original security reports that Recipient has undertaken or commissioned to assess Recipient's own network security. If requested, copies of these reports will be sent via bonded courier to the Exelon. Recipient will notify Exelon of any such security reports or similar assessments once they have been completed. Any regulators of Exelon or its Affiliates will have the same rights of audit as described herein upon request.

ARTICLE 11 - CYBER SECURITY INCIDENT / NETWORK SECURITY INSURANCE

Recipient will provide and maintain Cyber Security Incident/Network Security Insurance with a limit of not less than ten million dollars ($10,000,000) per occurrence and in the aggregate. Coverage will include liability for financial loss resulting from or arising out of Recipient's acts, errors, or omissions when accessing, processing, storing or transmitting Exelon Electronic Confidential Information, including: (i) breaches of Exelon'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; (v) denial or loss of service attacks; (vi) Internet advertising and content offenses; and. Such insurance will address all of the foregoing, without limitation, if caused by Recipient or Recipient Representatives in accessing, processing, storing or transmitting Exelon Electronic Restricted Confidential Information. 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.