TRADE ALLY REQUIREMENTS

The Trade Ally will be obligated to comply with the following in becoming a Trade Ally and providing work for customers under the Program:

1. **INFORMATION AND DATA**: The Trade Ally will maintain any customer information including name, account numbers, electric & natural gas consumption data and electric & natural gas energy savings it obtains in performing work for customers under the Program (the "Confidential Information") in strict confidence. This means that the Trade Ally will treat and cause to be treated as confidential and proprietary all Confidential Information in its possession. In furtherance thereof, the Trade Ally will: (a) take commercially reasonable steps to consistent with industry practices and the Trade Ally's published privacy policies to prevent the disclosure of Confidential Information except as permitted by herein or otherwise agreed to in writing by the customer; (2) use or process Confidential Information only in connection with the performance of the work for the customer under the Program; (3) make copies of any Confidential Information only as necessary for the performance of such work; (4) disclose Confidential Information only to personnel of the Trade Ally who have a need to know the Confidential Information in connection with the performance or use of such work; and (5) destroy the Confidential Information to promptly following the request of TRC or ACE, and in any event upon completion of all the Trade Ally's obligations under the Program. Participants in the program must comply with the terms and conditions regarding data security set by ACE within Attachment A.

2. **INSTALLATION REQUIREMENTS**: All work provided to customers under the Program by the Trade Ally must be in full compliance with the requirements of applicable laws, rules, and regulations of authorities having governmental and regulatory jurisdiction. Additionally, such work must be completed within 180 days of the commitment execution date on the agreement between the Program customer and the Trade Ally. In the removal of old equipment, the Trade Ally confirms that, as a requirement of the Program, Trade Ally will remove and dispose of, or confirm that the customer has done so, any and all equipment or materials that are replaced or removed in accordance with all applicable laws, rules, and regulations. If these requirements are not met, then ACE may cancel, withdraw, and revoke Trade Ally membership.

3**. INDEMNIFICATION:** The Trade Ally will, to the fullest extent permitted by law or regulation, defend, indemnify and hold harmless each of ACE and TRC, and all their respective subsidiaries or affiliates, their respective directors, officers, employees, agents and representatives ("Indemnitees") from and against any and all liabilities, losses, claims, damages, fines, penalties, costs, expenses (including reasonable attorney's fees), demands and causes of actions of every kind or character ("Losses") arising, or alleged to have arisen, out of any claims (just or unjust) relating to: personal injury, including death to any employee or other person; damage or injury to property, including loss of use; or a breach or incident to the performance of work under the Program and/or the acts or omissions of the Trade Ally, its employees and/or subcontractors. Notwithstanding the foregoing, the Trade Ally's obligations under this section will not extend to Losses that are the direct result of a fully adjudicated finding of negligence or intentional misconduct of an Indemnitee.

4. **PREVAILING WAGE AND PUBLIC WORKS**: If the work to be performed by the Trade Ally qualifies as a "public work" under the New Jersey State Prevailing Wage Act, N.J.S.A. 34:11-56.25 et seq. (the "Act"), the Trade Ally agrees to adhere to and comply with the Act and shall require the same of its subcontractors. These obligations include but are not limited to: 1) workers employed in the performance of work under the Program shall be paid not less than the prevailing wages applicable, and 2) the Trade Ally will employ on the site only individuals who have successfully completed all OSHA-certified safety training, if any, required as a prerequisite for the particular work to be performed under the Program. If the work falls under the jurisdiction of the New Jersey Division of Property Management and Construction, The Trade Ally agrees to comply with and to require its subcontractors to comply with all requirements of that agency and any related law.

5**. LIMITATION OF LIABILITY**: BY PARTICIPATING AS A TRADE ALLY FOR THE PROGRAM, THE TRADE ALLY AGREES TO WAIVE ANY AND ALL CLAIMS, WHETHER ARISING IN CONTRACT OR TORT AND TO FULLY RELEASE ACE AND TRC, AND THEIR RESPECTIVE REPRESENTATIVES,OFFICERS, DIRECTORS, EMPLOYEES, AFFILIATES, CONTRACTORS AND AGENTS FROM ANY AND ALL DAMAGES, OF ANY KIND. IN NO EVENT WILL ACE OR TRC, OR THEIR RESPECTIVE REPRESENTATIVES, OFFICERS, DIRECTORS, EMPLOYEES , AFFILIATES, CONTRACTORS OR AGENTS, UNDER ANY CIRCUMSTANCES, BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL LOSSES INCLUDING, BUT NOT LIMITED TO, DAMAGES RELATED TO SAFETY, HEALTH OR WELL-BEING, LOST OR REDUCED PROFITS, REVENUES, EFFICIENCY, PRODUCTIVITY, BONDING CAPACITY, OR BUSINESS OPPORTUNITIES, OR INCREASED OR EXTENDED OVERHEAD, OPERATING, MAINTENANCE, OR DEPRECIATION COSTS AND EXPENSES.

6**. WARRANTIES**: In providing work for customers under the Program, the Trade Ally will warrant that: (a) all work provided by will: (i) be of high quality; (ii) be free from any defects; (iii) be suitable for the purposes for which it was intended; (iv) be properly installed; (v) result in dependable service and performance as specified in, or that may reasonably be inferred from, the Program requirements or the agreement with the customer; (vi) comply with established industry codes and standards; (vii) comply with sound industry and work practices; (viii) comply with all laws; (ix) not violate any intellectual property right or other proprietary interest; and (x) otherwise fully conform in all respects to the Program requirements or the agreement with the customer; (b) all material provided to the customer, including all components incorporated into the work, will be new and free from any liens, encumbrances, security interests, and defects in title; (c) any system(s) provided as part of the work (including but not limited to heating, wiring, piping, cooling, plumbing, electrical, control, lighting, alarm, or computer systems) will operate properly and dependably and be compatible with other existing or connecting systems; (d) any material provided as part of such system(s) shall be compatible with the system(s) and its components; (e) during the progress of the work , the Trade Ally will, at its sole cost and expense, promptly repair, replace, or re-perform any work, including material, in whole or in part, that is rejected by ACE or TRC as failing to conform to the Program requirements, and the Trade Ally will also bear all expenses required to fix

any work under the Program that is impaired, destroyed, or damaged by such non-conforming work or the repair, replacement, or re-performance of such non-conforming work;
and (f) for one year from the date work has been placed into commercial use (the "Warranty Period"), the Trade Ally will promptly repair, correct, replace, and re-perform any said work that fails to conform to the Program requirements or the agreement with the customer at no additional cost to the customer and all such warranty work will be performed on a schedule acceptable to the customer and will be warranted for one (1) additional full year from the date of repair, correction, replacement, or reperformance of such work, which one (1) additional year shall be considered the Warranty Period; in addition, the placement of such work into commercial use will not relieve the Trade Ally of its responsibility to provide conforming work.

Further in providing work for customers under the Program: (a) written communication to the Trade Ally from the customer, ACE or TRC specifying defective or otherwise nonconforming work that appears either during the progress of the work or during the Warranty Period after placement of the into commercial use will be deemed sufficient notice to the Trade Ally to promptly remedy the defect or nonconformity as required under the Program requirements and the agreement with the customer; (b) if repair, correction, replacement, or reperformance of defective or otherwise nonconforming work by the Trade Ally would, in ACE's, TRC's or the customer's opinion, be impracticable or disadvantageous to the customer, the customer will be entitled to a full refund of the price paid by the customer for such defective or nonconforming work; (c) the liability of the Trade Ally will extend to all of customer's damages caused by the breach of any of the foregoing warranties and shall include, but not be limited to, the cost of removal and replacement of nonconforming material, shipping of material, correction of work, the customer's expenses resulting from the breach of the warranty, and the cost of removal and reinstallation of other material or work made necessary thereby; and

(d) the Trade Ally will identify to the customer in writing all third-party or original equipment manufacturer warranties that the Trade Ally receives in connection with the work and will pass through to the customer the benefits of all such warranties (the "Pass-Through Warranties"); provided, however, that nothing in this section will reduce, or limit, or expand the Trade Ally's obligations under the Program or the agreement with the customer.

7. **INSURANCE REQUIREMENTS**: By participating as a Trade Ally under the Program, the Trade Ally agrees to provide and maintain in effect during the duration of its tenure as a Trade Ally the following minimum insurance coverage with carriers authorized to conduct business in the State of New Jersey, including: (a) Workers Compensation insurance ("WCI") with statutory limits, as required by the State of New Jersey; (b) Employer's liability insurance ("ELI") with limits of not less than $1,000,000.00 each accident for bodily injury by accident, each employee for bodily injury by disease, and policy limit; (c) Commercial general liability ("CGL") insurance (with coverage consistent with ISO Form CG 00 0104 13 or its equivalent with a limit of not less than $1,000,000.00 per occurrence and per project or per location aggregate, covering liability for bodily injury and property damage, arising from premises, operations, independent contractors, personal injury/advertising injury, liability assumed under an insured contract and products/completed operations for not less than three years from the Program end date, or the last date the project for any customer served by the Trade Ally under the Program is placed into commercial use, whichever is later; (d) Automobile liability insurance ("ALI") coverage (including coverage for claims against the customer for injuries to personnel of the Trade Ally for owned, non-owned, and hired autos with a limit of not less than $1,000,000.00 per accident; and (e) Excess or Umbrella liability insurance coverage with a limit of not less than $4,000,000.00 per occurrence and per project or per location aggregate. These limits apply in excess of each of the above-mentioned policies. Excess coverage will be follow form. The liability limits under subsections (b), (c), (d) and (e) above may be met with any combination of primary and Excess or Umbrella Insurance policy limits totaling $5,000,000. If any policy is written on a claims made basis, the retroactive date may not be advanced beyond the Program start date and coverage will be maintained in full force and effect for three years from the Program end date, or the last date the project for any customer served by the Trade Ally under the Program is placed into commercial use, whichever is later, which coverage may be in the form of tail coverage or extended reporting period coverage if agreed by the Trade Ally and either TRC or ACE. The Trade Ally will be responsible for any deductibles or self-insured retentions applicable to the insurance provided in compliance with this section. To the extent permitted by applicable laws, all above-mentioned insurance policies will: (1) be primary and non-contributory to any other insurance afforded to the customer, ACE or TRC; (2) contain cross-liability coverage as provided under standard ISO Forms' separation of insureds clause; (3) provide for a waiver of all rights of subrogation which the Trade Ally's insurance carrier might exercise against the customer, ACE or TRC (excluding PLI); (4) not require contribution before any Excess or Umbrella liability coverage will apply; and (5) having ratings of A-/VII or better in the Best's Key Rating Insurance Guide (latest edition in effect at the latest date stated in the Certificate of Insurance. All liability insurance policies (excluding PLI and WCI) will include the ACE as an additional insured, will be primary to any other insurance carried by the customer, and will provide coverage consistent with ISO Form CG 2026 (11/85), or the combination of ISO Form CG 20 10 04 13 and CG 20 37 04 13, or their equivalents, and will maintain the required coverages, for a period of not less than three years from the Program end date, or the last date the project for any customer served by the Trade Ally under the Program is placed into commercial use, whichever is later. The Trade Ally will provide evidence of the required insurance coverage and file with TRC a Certificate of Insurance acceptable to TRC prior to commencement of any work under the Program. The Trade Ally will provide written notification to TRC if the policies required by this section are canceled, allowed to expire or the limits materially reduced with at least 30 days prior written notice ten business days in the case of nonpayment of premium).

8. By participating as a Trade Ally under the Program, the Trade Ally agrees, in addition to complying with all other Program requirements, to be subject to the Contractor Remediation Policy attached as Attachment B, which was agreed to by the seven investor-owned utilities in New Jersey. For purposes of clarity, references to "Contractor" in the Contractor Remediation Policy will have the same meaning as Trade Ally.

ATTACHMENT A

BASIC CYBER AND INFORMATION SECURITY REQUIREMENTS

ARTICLE 1 - SCOPE

1.1 If the Trade Ally will access, process, store or transmit the Confidential Information (as defined in the Agreement), it will adhere to the requirements of this Attachment A.

1.2 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 Trade Ally personnel, contractors, and third-party personnel, including suppliers, that have been granted authorized access to the Confidential Information.

"**Account ID**" means any identification name or code associated with 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).

"Affiliate" means persons or entities 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 Trade Ally's electronic systems.

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

"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.

"Cyber Security Incident" means any malicious act or suspicious event, or group of suspicious events occurring during the performance of, or in connection with the work provided by the Trade Ally under the Program, that is a Compromise, or has or had the potential to be a Compromise, of: (1) Electronic Confidential Information stored or transmitted on Trade Ally's Electronic Information Assets; or (2) violates a cyber security or information security requirement herein, or under Cyber Security Laws, including when:

(a) The Trade Ally knows or reasonably believes that there has been a Compromise of Electronic Confidential Information hosted or stored by the Trade Ally;

(b) The Trade Ally knows or reasonably believes that there has been a Compromise of the physical, technical, administrative, or organizational safeguards protecting the Trade Ally's Electronic Information Assets accessing, processing storing or transmitting Electronic Confidential Information; or

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

(i) The Trade Ally's handling of Electronic Confidential Information; or

(ii) The Trade Ally 's compliance with the cyber security or information security requirements herein or applicable Cyber Security Laws in connection with the Electronic Confidential Information; or

"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 Electronic Confidential 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).

"Disaster Recovery Plan" means a disaster recovery plan set forth in Article 12 (Disaster Recovery and Business Continuity).

"Electronic Confidential Information" means Electronic Information which is 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).

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

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

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

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

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

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

"**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 to customers under the Program.

"Physical Security Controls" mean policies, standards and procedures designed to prevent unauthorized physical access, damage, and interference to Electronic Confidential Information and the Trade Ally's Electronic Information Assets.

"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.

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

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

"**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) customers under the Program or (2) transmission and distribution systems, as further defined in various state Laws.

"**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.

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

"**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, 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 2 - TRADE ALLY'S INFORMATION SECURITY PROGRAM

3.1 The Trade Ally will document, implement, and maintain an Information Security Program to protect the integrity, availability, and confidentiality of Electronic Confidential Information in accordance with the requirements set forth in this Attachment A.

3.2 The Trade Ally will train its personnel with access to Electronic Confidential Information on the key elements of the Trade Ally's Information Security Program so that they understand their responsibilities for the secure handling of Electronic Confidential Information.

3.3 The Trade Ally will provide annual information security awareness refresher training to its personnel who have access to Electronic Confidential Information. Training will include the Trade Ally's Information Security Program and standards for the secure handling of Electronic Confidential Information.

ARTICLE 3 - TRADE ALLY'S ACCESS MANAGEMENT PROGRAM

4.1 The Trade Ally will only grant access to the Trade Ally Electronic Information Assets where Electronic Confidential Information is processed, stored, or transmitted to its personnel who need access in order to perform the work for customers under the Program and will revoke such access promptly once the person no longer requires or is no longer qualified for access.

4.2 The Trade Ally will assign each individual personnel a unique User Account ID for which the Trade Ally will be responsible for all activities performed under that User Account ID.

4.3 The Trade Ally will limit Administrator Account access to Electronic Confidential Information being processed, stored or transmitted using the Trade Ally's Electronic Information Assets to only those personnel whose job role and responsibilities require such access.

4.4 The Trade Ally 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 The Trade Ally will prohibit its personnel to share or otherwise allow other persons to use their unique User Account IDs and associated passwords and terminate access to Electronic Confidential Information for its personnel who violate this prohibition.

4.6 The Trade Ally will immediately remove its personnel's access to any Electronic Confidential Information and its Electronic Information Assets where 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, (iii) the services being provided by the Trade Ally to customers under the Program are either completed or terminated, or (iv) when the Trade Ally reasonably believes the individual may pose a threat to the safety or security of Electronic Confidential Information.

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

ARTICLE 4 - TRADE ALLY'S DATA BACKUP OF ELECTRONIC CONFIDENTIAL INFORMATION

5.1 The Trade Ally will develop, implement, maintain, review and monitor a Data Backup Plan to protect the confidentiality, integrity, and availability of 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 5 - TRADE ALLY'S USE OF CRYPTOGRAPHY

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

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

ARTICLE 6 - TRADE ALLY'S CYBER SECURITY INCIDENT REPORTING, RESPONSE & RECOVERY

7.1 The Trade Ally will document, implement, and maintain a Cyber Security Incident Management Process to protect the confidentiality, integrity and availability of Electronic Confidential Information.

7.2 The Trade Ally'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 The Trade Ally will immediately inform ACE and TRC upon becoming aware of any Cyber Security Incident.

7.4 The Trade Ally will immediately provide a verbal report of any Cyber Security Incidents to the Exelon Security Operations Center ("ESOC") by telephone (to 1-800-550-6154, international at 410-470-5800), and follow up by email (to ESOC@exeloncorp.com). The report will include the date and time of the occurrence of the Cyber Security Incident (or the approximate date and time of the occurrence if the actual date and time of the Cyber Security Incident is not precisely known) and a detailed summary of the facts and circumstances of the Cyber Security Incident, including a description of (a) why the Cyber Security Incident occurred, and (b) the measures being taken to address and remedy the Cyber Security Incident to prevent the same or a similar event from occurring in the future. The Trade Ally will provide written updates of the notice to ESOC 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.

7.5 Within ten (10) days of notifying ESOC of the Cyber Security Incident, the Trade Ally will recommend actions to be taken by the Trade Ally 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. The Trade Ally will coordinate with ESOC in developing those action plans and mitigating controls.

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

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

ARTICLE 7 - TRADE ALLY'S SECURITY PATCH MANAGEMENT

8.1 The Trade Ally 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 The Trade Ally 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 The Trade Ally 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. The Trade Ally will promptly notify ESOC of any Vulnerability that cannot be effectively closed by a Security Patch or other corrective action by the Trade Ally and will document and implement appropriate mitigating technical controls to protect Electronic Confidential Information.

ARTICLE 8 - TRADE ALLY'S PASSWORD MANAGEMENT

9.1 The Trade Ally will ensure that the Trade Ally's Electronic Information Assets which access, process, store, or transmit Electronic Confidential Information employ strong password complexity rules.

9.2 The Trade Ally will require all its personnel to comply with the Trade Ally'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 The Trade Ally 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 9 - TRADE ALLY'S PHYSICAL SECURITY

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

10.2 The Trade Ally will ensure its Electronic Information Assets in which the Electronic Confidential Information are stored are appropriately secured from unauthorized physical access.

10.3 The Trade Ally will maintain all backup and archival media containing the Electronic Confidential Information in secure, environmentally controlled storage areas owned, operated, or contracted for by the Trade Ally.

10.4 The Trade Ally will have processes and procedures for the control and monitoring of visitors' and other external persons' physical access to the Trade Ally's Electronic Information Assets on which the 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 10 - TRADE ALLY'S MALWARE PROTECTION

11.1 The Trade Ally will deploy industry-standard Malware protection software on all its Electronic Information Assets that access, process, store or transmit the Electronic Confidential Information.

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

ARTICLE 11 - CYBER SECURITY INCIDENT / NETWORK SECURITY INSURANCE

The Trade Ally will provide and maintain Cyber Security Incident/Network Security Insurance with a limit of not less than five million dollars ($5,000,000) per occurrence and in the aggregate. Coverage will include liability for financial loss resulting from or arising out of acts, errors, or omissions in the performance of contractual obligations assumed by the Trade Ally under the Program, including: (i) violation of any right to privacy or privacy Laws; (ii) Cyber Security Incidents and violation of any Cyber Security Laws; (iii) data theft, damage, destruction, or corruption, including unauthorized access, unauthorized use, identity theft, theft of confidential corporate information, transmission of a computer virus or other type of malicious code; and (iv) denial or loss of service attacks, including ransomware attacks; (v) Internet advertising and content offenses; (vi) defamation; (viii) errors or omissions in software or systems development, implementation and maintenance. Such insurance will address all of the foregoing, without limitation, if caused by the Trade Ally in performing the work for customers under the Program. This 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 12 - DISASTER PREPAREDNESS AND BUSINESS CONTINUITY

12.1 The Trade Ally will document, implement, and maintain a Business Continuity Plan to protect the privacy, confidentiality, integrity, and availability of Electronic Confidential Information and Trade Ally's Electronic Information Assets.

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

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

12.3.1 The Trade Ally will back-up and store the Electronic Confidential Information (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.

12.3.2 The Trade Ally will encrypt the Electronic Confidential Information when being transmitted electronically by the Trade Ally or stored on the Trade Ally's Electronic Information Assets.

12.3.3 The Trade Ally will conduct incremental and full back-ups (in accordance with the Disaster Recovery Plan) to capture data, and changes to data used in connection with the work performed by the Trade Ally for customers under the Program. Backed up data will be encrypted.

12.3.4 The Trade Ally will develop, maintain and submit a Disaster Recovery Plan to ACE and TRC, including plans, measures and arrangements to ensure the continuous delivery of critical products and services, which permits the Trade Ally to recover its facility, data, assets and personnel.

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

12.3.4.2 The Trade Ally will generate a report following each and any disaster measuring performance against the Disaster Recovery Plan and identification of problem areas and plans for resolution.

12.3.5 The Trade Ally's Business Continuity Program documentation will be made available to ACE and TRC upon request.

ATTACHMENT B
CONTRACTOR REMEDIATION POLICY

New Jersey Energy Efficiency Programs Joint Utility Contractor Remediation Policy

As part of the transition anticipated by the 2018 Clean Energy Act ("CEA"), the seven (7) investor-owned utilities in New Jersey[1] (each, a "Utility") will be assuming primary responsibility for many of the Energy Efficiency Programs ("Programs") previously administered by the State of New Jersey and will be launching new Programs in an effort to meet the energy reduction targets required by the CEA. The Board of Public Utilities ("BPU") has further established requirements for the utilities to adopt a coordinated contractor remediation policy for Programs.[2] All contractors participating in any of the Utility Programs should be familiar with this policy and understand the consequences for failure to comply.

General Requirements

In order to participate in the Programs, Contractors must:

- Carefully review, understand and comply with the requirements of all Programs that they participate in.
- Hold a valid New Jersey license for all contractor work performed and continue to meet all underlying requirements for the respective licenses for the types of work they are performing.
- Secure permits when required.

Minor Infractions

Each Utility, or its implementation contractor, will monitor contractor performance. Minor infractions regarding Program rules, as determined in the sole discretion of the applicable Utility or implementation contractor, will be corrected and/or investigated. Examples of minor infractions, include but are not limited to:

- Unintentionally incorrect or incomplete data submittals;
- Unintentionally incorrect or incomplete equipment ratings; or
- Evidence, including legitimate customer complaints, of:
    - Deficient service and/or equipment; or
    - Misleading sales or commercial practices.

Contractors will be notified regarding minor infractions identified, along with planned remediation strategies, which may include but are not limited to coaching, additional written guidance, an increased level of quality assurance/quality control/inspections performed on their projects and/or required training or retraining.

Repeated minor infractions may be escalated to be considered as a major infraction if a contractor has not taken action to address the underlying problems causing such infractions despite the remediation actions taken. Any infraction that poses a significant threat to human health and safety will automatically be considered a major infraction.

[1] The seven Investor-Owned Utilities include Atlantic City Electric Company, Elizabethtown Gas Company, Jersey Central Power and Light Company, New Jersey Natural Gas Company, Public Service Electric and Gas Company, Rockland Electric Company, and South Jersey Gas Company.

[2] As defined in the BPU's June 10, 2020 Order in Docket Nos. QO19010040, QO19060748, and QO17091004.

Major Infractions

Each Utility, or its implementation contractor, will monitor contractor performance and share evidence of major infractions with the other Utilities. Major infractions regarding Program rules will be corrected and/or investigated. Examples of major infractions include, but are not limited to:

- Any actions that pose a significant threat to human health and safety;
- Evidence of intentionally incorrect or incomplete data submittals;
- Evidence of intentionally incorrect or incomplete equipment ratings;
- Evidence of dishonesty, fraud, deception, misrepresentation, false promise or false pretense;
- Evidence the contractor has engaged in repeated acts of negligence, submissions of incorrect or incomplete data, significantly deficient service, unethical, misleading, or illegal sales or commercial practices, or other failures to meet standards of business conduct and/or professional standards required under their licensing or technical requirements;
- Evidence the contractor has been convicted of, or engaged in acts constituting, any crime or offense involving moral turpitude or relating adversely to the contractor's business. For the purpose of this subsection, a judgment of conviction or a plea of guilty, *non vult*, *nolo contendere*, or any other such disposition of alleged criminal activity, shall be deemed a conviction; or
- Evidence that any of the contractor's personnel is presently engaged in drug or alcohol use that is likely to impair such personnel's ability to conduct contractor's business with reasonable skill and safety. For purposes of this policy, the term "presently" means at this time or any time within the previous three hundred sixty-five (365) days;
- Repeated minor infractions without , signs of improvement, as determined by a majority of the Utilities;
- Misrepresentation within the contractor's participation agreement (where applicable); or
- Violation of New Jersey licensing requirements.

Contractors will be notified in writing of major infractions identified by a Utility (or determined by a majority of the Utilities, as applicable), along with planned remediation strategies, which may include but are not limited to probation, suspension, or disbarment from the Programs. For the purposes of this policy, these actions shall be defined as:

Probation: Defined period of days where every pending Program project for that contractor will be inspected before issuing payment and all applications pending will require pre-approval from a Manager or higher for all Programs for all Utilities.

Suspension: Defined period of days where the contractor will be prohibited from submitting any new applications to any Program or participating in any new Program customer application as a subcontractor. Existing applications that are in process and deemed complete prior to the suspension will be allowed to proceed; provided however that the Utilities will have the right but not the obligation to inspect up to100% of the contractor's remaining projects. A contractor that has been suspended is precluded from using any Utility forms or software.

Disbarment: Contractor is prohibited from participation in any Program for any of the Utilities.

While an individual Utility will identify the major infraction for the contractor, all Utilities will be notified of the circumstances and will collectively decide, by a majority, the appropriate remediation strategy, which will be applied across all Utility service territories. A contractor will have five (5) business days from the date the notice of action is issued to provide a response if it believes there are extenuating circumstances that merit reconsideration of the notice of action. The Utilities will provide a collective response within ten (10) business days and either confirm initial remediation action or address modified response.