I. Introduction
The Smart Grid is a planned nationwide network that uses information technology to deliver electricity efficiently, reliably, and securely. A key element of the Smart Grid, Smart Meters, enable more detailed collection of customer energy usage to help utilities manage the delivery of energy more effectively. This detailed data, when made available to customers, enables them to understand their energy use and manage it more economically. Companies that provide services such as home security management systems, smart thermostats, smart appliances, energy management apps, and other services can also use this data. Companies offering these services need access to energy data, data that the utility companies have not traditionally shared, to provide their services.

Companies seeking to access a consumer energy data must do so with clear customer consent. Companies seeking this data that has been collected by utilities must ensure utilities, regulators and customers that data will be handled responsibly. The TRUSTed Smart Grid Privacy Program helps companies certify their data collection and usage practices using a standard based on Smart Grid Guidelines developed by the Future of Privacy Forum and TRUSTe’s core values of transparency, choice, and accountability.

The TRUSTed Smart Grid Privacy Program is designed to certify privacy practices of companies seeking to access customer energy usage data [CEUD] that is collected by utilities via the utilities direct relationship with the customer. The program will also certify companies collecting energy data directly from customers through smart devices such as smart thermostats, smart appliances or home control systems. This program is not designed to include collection of CEUD by the utilities from their smart meters or companies acting as service providers under control of a utility or third party.

II. Structure
TRUSTe privacy certification programs are comprised of Program Requirements that define a compliance standard for business practices involving the collection and use of data. To obtain TRUSTe certification, a company must provide proof of its privacy and data governance practices for data collected from users – particularly as these practices relate to notice, choice, and accountability. Upon satisfactory evaluation, TRUSTe provides a trustmark indicator - typically in the form of a seal or whitelist placement - that certifies the company’s practices are compliant with TRUSTe’s privacy standard.

III. Definitions
The following definitions shall apply herein:

A. “Clear and Conspicuous” means a notice that is reasonably easy to find, and easily understandable in terms of content and style to the average reader.

B. “Customer Energy Usage Data [CEUD]” means energy usage information and data identifiable to an individual customer obtained through the use of advanced metering infrastructure, from the home area network, or from other devices.

C. “Expressed Consent” means the affirmative consent (opt-in) to a practice by the Individual, after being provided notice, but prior to implementing the practice,

D. “Foreign Language Privacy Statement” is the Participant’s Privacy Statement translated into a language other than English.
E. “Geo-location Data” is information obtained through an Individual’s use of a Mobile Device and is used to identify or describe the Individual’s actual physical location at a given point in time.

F. “Individual” means the discrete person to whom the collected information pertains.

G. “Inferred Consent” means consent which is implied by an Individual, regarding the collection, use, disclosure, distribution of PII after notice and opportunity to withdraw consent (opt-out) is given by Participant, but not taken by the Individual.

H. “Material Change” means degradation in the rights or obligations regarding the collection, use, or disclosure of CEUD containing PII or PII for an Individual. This usually includes changes to Participant’s:
   1. Practices regarding notice, collection, use, and disclosure of CEUD containing PII, PII, or PII collected from someone other than the Individual to whom the PII pertains;
   2. Practices regarding user choice and consent to how CEUD containing PII, PII, or PII collected from someone other than the Individual to whom the PII pertains is used and shared; or
   3. Measures for information security, integrity, access, or individual redress.

I. “Mobile Device” is a portable electronic geo-location enabled device that allows the user to process, receive, and send data without being limited to a specific geographical location.

J. “Online” is the state where an Individual is connected by computer, Mobile Device, or Smart Device to one or more other computers, Mobile Devices, Smart Devices, or networks, as through a commercial electronic information service or the internet.

K. “Participant” means the entity that has entered into an agreement with TRUSTe to participate in the TRUSTe program(s) and agreed to comply with the program requirements included therein.

L. “Personally Identifiable Information [PII]” means any information or combination of information that can be used to identify, contact, or locate a discrete Individual.

M. “Primary Purpose” means use of PII that is reasonably expected by the Individual (i) at the point of collection; and (ii) including compatible uses in features and services to the Individual that do not materially change expectations of user control and third party sharing. Such use may be at least those uses described in the Participant’s terms of service governing the Participant’s products or services which give rise to the Individual’s interaction with the Participant.

N. “Privacy Statement” shall mean the statements of Participant’s information collection and use practices, as such practices are updated from time to time. Participant's Privacy Statement includes, but is not limited to:
   1. A single, comprehensive statement of all the Participant's information practices ("Comprehensive Privacy Statement");
2. A summary notice highlighting the Participant’s information practices ("Short Notice"); or

3. Disclosure of specific information practices posted at the point of information collection ("Just in Time Notice").

O. "Secondary Purpose" is the use of PII that is materially different from the Primary Purpose and is not reasonably expected by the Individual relative to the transactions or ongoing services provided to the Individual by Participant or the Participant’s Service Provider.

P. "Service Provider" is anyone other than the Participant, Utility, or the Individual that performs, or assists in the performance of, a function or activity, which may involve the use or disclosure of PII or PII collected from an entity other than the Individual to whom the PII pertains. Such use must only be on behalf of Participant, Utility, or Individual and only for the purpose of performing or assisting in that specific function or activity as agreed to by the Individual, and Participant or Utility.

Q. "Smart Device" for the purposes of this program is a device, system, program, app, or similar technology that can collect and transmit information about an individual’s energy use or other individual activity.

R. "Third Party(ies)" is an entity(ies) other than the Participant or the Individual which is not directly affiliated with the Participant; and, if affiliated with the Participant, where such affiliation is not reasonably known to the Individual.

IV. Minimum Program Requirements

A. All Participants wanting to be certified that their Online information collection and use practices comply with TRUSTe’s TRUSTed Smart Grid Privacy Program Requirements must comply with the following requirements:

B. Participant Accountability

1. Participant shall have processes in place to comply with these Program Requirements.

2. Cooperation with TRUSTe

a) Provide, at no charge to TRUSTe or its representatives, full access to the Online properties (i.e., including password access to premium or members only areas) for the purpose of conducting reviews to ensure that Participant's Privacy Statement(s) is consistent with actual practices.

b) Provide, upon TRUSTe’s reasonable request, information regarding how PII gathered from and/or tracked through Participant's Online properties is used.

3. Annual Recertification

a) Participant shall undergo re-certification to verify ongoing compliance with these Program Requirements annually.
4. **Termination for Material Breach**
   
a) In the event TRUSTe reasonably believes the Participant has materially breached these Program Requirements, TRUSTe may terminate the Participant’s participation in this program upon twenty (20) business days’ prior written notice (“Notice of Termination”) unless the breach is corrected within the same twenty (20) business day period (“Cure Period”).

b) Material breaches of these Program Requirements include but are not limited to:

   1. Participant’s continual, intentional, and material failure to adhere to these Program Requirements;
   
   2. Participant’s material failure to permit or cooperate with a TRUSTe investigation or review of Participant’s Online properties or practices pursuant to the Program Requirements;
   
   3. Participant’s continual, intentional, and material failure to comply with any Suspension Obligations;
   
   4. Participant’s material failure to cooperate with TRUSTe regarding an audit, complaint or the compliance monitoring activities of TRUSTe; or
   
   5. Any deceptive trade practices by the Participant.

5. **Suspension Status**

a) In the event TRUSTe reasonably believes that Participant has materially violated these Program Requirements, Participant may be placed on suspension.

   1. Notice will be provided with a mutually agreed upon description of the violation and any remedial actions that TRUSTe will require Participant to take during the Suspension Period (“Suspension Obligations”).

   2. Participant will be considered to be on Suspension immediately upon receiving notice from TRUSTe. Suspension shall last until such time as the Participant has corrected the material breach or Program Requirements violation to TRUSTe’s satisfaction, but not for a period of greater than six (6) months (“Suspension Period”) unless mutually agreed by the Parties.

   3. Suspension Obligations may include, but are not limited to:

      a) Compliance with additional Program Requirements;
      
      b) Cooperation with heightened compliance monitoring by TRUSTe; and
(c) Payment to TRUSTe of mutually agreed additional amounts as compensation for TRUSTe’s additional compliance monitoring.

(d) Participant shall comply with all Suspension Obligations.

(4) During the Suspension Period, Participant’s status may be indicated via a TRUSTe Validation webpage or TRUSTe may require Participant to cease using the TRUSTe trustmarks.

(5) At the end of the Suspension Period, TRUSTe will, in its discretion, either:

(a) Determine that Participant has complied with Participant’s Suspension Obligations, thereby satisfying TRUSTe’s concerns;

(b) Extend the Suspension Period by mutual agreement with the Participant; or

(c) Determine that Participant has failed to comply with Participant’s Suspension Obligations and immediately terminate Participant for cause.

C. Privacy Practices

The following requirements apply if the Participant collects CEUD and/or PII (except to the extent that the Participant acts as a Service Provider of the utility that collects CEUD and/or PII):

1. Collection Limitation

   a) Participant shall only collect or receive CEUD containing PII with notice to and consent of the Individual.

      (1) Any Just-in-Time Notice shall explain key collection and use practices that are relevant to and needed by the Individual to provide consent prior to the collection of CEUD containing PII.

   b) Participant shall only collect PII where such collection is:

      (1) Limited to information reasonably useful for the purpose for which it was collected and in accordance with the Participant’s Privacy Statement in effect at the time of collection; or

      (2) With notice to and consent of the Individual.

2. Use of CEUD and/or PII

   a) Participant shall use CEUD and/or PII in accordance with their notice, and in accordance with their posted Privacy Statement in effect at the time of collection, or with notice and consent as described in these Program Requirements.
b) Participant may collect data and de-identify it for use as anonymous individual data and anonymous aggregate data provided a recipient of the data could not reasonably link the data to a specific Individual or an Individual’s household.

c) Participant shall aggregate and/or anonymize CEUD if CEUD does not need to be used or maintained in a personally identifiable form prior to transmission to Third Parties.

d) Information collected by the Participant or the Participant’s Service Provider may be used to tailor the Individual’s experience on the Participant’s Online property.

3. Choice

a) Participant shall offer the Individual control over their information as follows:

   (1) Participant must provide the Individual an opportunity to withdraw consent to having PII not containing CEUD used by the Participant or shared with Third Parties other than Service Providers for a Secondary Purpose.

   (2) Participant must provide the Individual an opportunity to withdraw consent to having PII containing CEUD used by the Participant for a Secondary Purpose.

   (3) Participant must obtain the Individual’s Express Consent prior to the disclosure, distribution, or transfer of CEUD containing PII to Third Parties, other than Service Providers;

   (4) Participant shall honor and maintain the Individual’s choice selection in a persistent manner until such time the Individual changes that choice selection; and

   (5) Participant shall provide a means by which the Individual may change their choice selection.

b) Consent is not necessary when CEUD containing PII and/or PII is:

   (1) Used for operational purposes to provide requested services;

   (2) Disclosed to Service Providers; or

   (3) Where the use, disclosure or distribution of CEUD containing PII and/or PII is required by law, court order, or other valid legal process.

c) Privacy Statement shall state when the Individual can exercise control over the use and sharing of their CEUD containing PII or PII and how to exercise that control.

d) Such mechanism shall be easy to use and offered at no cost to the Individual.
4. Access

a) Participant must provide Individuals with reasonable and appropriate mechanisms to access their own CEUD.

b) Participant must implement reasonable and appropriate mechanisms to allow the Individual to correct or update inaccurate PII.

c) Participant must implement reasonable mechanisms to allow the Individual to request deletion of CEUD or PII, or that collected PII no longer be used.

d) Such mechanism should be consistent with how the Individual normally interacts or communicates with the Participant.

e) Such mechanism or process shall be clear, conspicuous, and easy to use.

f) Mechanisms or processes described above shall confirm to the Individual inaccuracies have been corrected; and

g) Participant’s privacy statement shall state how access is provided.

h) Participant is not required to permit Individual access to CEUD or PII to the extent that:

   (1) Such access would prejudice the confidentiality necessary to comply with regulatory requirements, or breach Participant’s confidential information or the confidential information of others;

   (2) The burden or cost of providing access would be disproportionate or the legitimate rights or interests of others would be violated. However, Participant may not deny access on the basis of cost if the Individual offers to pay the costs of access; or

   (3) The requested PII is derived from public records or is Publicly Available Information and is not combined with non-public record or non-publicly available information.

i) If Participant denies access to CEUD or PII, Participant must provide the Individual with an explanation of why access was denied and contact information for further inquiries regarding the denial of access.

5. Promotional and Newsletter Email Communications

a) All newsletters and promotional email messages that Participant sends to the Individual must include Participant’s postal address and a functional unsubscribe mechanism.
b) The location and instructions concerning the unsubscribe mechanism must be Clear and Conspicuous, and the mechanism itself must be functional for no fewer than thirty (30) days following the sending of the newsletter or promotional email message.

c) Participant must honor the Individual’s request to unsubscribe from a newsletter or promotional email message beginning on the tenth (10) business day after the Participant receives the unsubscribe request, unless the Individual subsequently requests to receive newsletters or promotional email messages from Participant.

d) An unsubscribe mechanism is not required for administrative or customer service-related email messages (e.g. account management or provisioning of requested services, warranty or recall information, safety or security announcements).

6. Public Disclosure of PII

a) A Participant may allow a user to post PII in an online forum, chat room, blog or other public forum, where the PII being displayed was placed there by a user who is also the Individual.

   (1) If appropriate and commercially reasonable, provide a process or mechanism to allow the Individual to request timely removal of any publicly displayed PII where it has been legally and rightfully shared; and

   (2) State in the Privacy Statement how the Individual can request removal of publicly displayed PII.

b) The Privacy Statement shall state information posted by Individuals in online forums, chat rooms, blogs, or other public forum may be displayed publicly.

c) The Privacy Statement shall accurately describe the extent to which an Individual's displayed PII is publicly available.

7. Material Changes

a) Participant must notify Individuals of any Material Changes to its collection, use, or disclosure practices for CEUD containing PII and/or PII prior to making the change.

b) Participant must obtain the Individual's Express Consent prior to implementing any Material Change to its, use, or disclosure practices for CEUD containing PII collection.

c) Participant may stop providing the Individual services or provide a different tier of service if the Individual does not consent to a Material Change in the Participant’s collection, use, and disclosure practices for CEUD containing PII.

   (1) Notice to the Individual regarding a Material Change shall disclose whether the Individual must forgo the service or their service tier changes if the Individual does not consent.
d) Participant must obtain prior approval from TRUSTe
   
   (1) For any Material Change in its collection, use, or disclosure practices for CEUD containing PII or PII; and
   
   (2) For method and notice to Individuals, such as email, “in product” messaging, etc.

D. Privacy Statement

1. Participant shall maintain and abide by an accurate up-to-date Privacy Statement approved by TRUSTe in its sole discretion that states Participant’s information practices and is in conformance with these Program Requirements including, but not limited to:

   a) What information is collected, either through active or passive means, type of entity(ies), excluding Service Providers, collecting the information, and how the collected information is used;

   b) What types of Third Parties if any, including Service Providers, collected information is shared with;

   c) Whether CEUD containing PII and/or PII is appended with information obtained from third party sources;

   d) How and when the Individual can exercise choice as required in these Program Requirements;

   e) How the Individual can request access to their information as required in these Program Requirements;

   f) What types of security measures are in place to protect collected information as required in these Program Requirements;

   g) What, if any, tracking technologies are used by the Participant or Third Parties including Service Providers and the purpose for using those technologies;

   h) How the Individual can contact the Participant, including company name, email address or a link to an online form, and physical address;

   i) How the Individual will be notified of any Material Changes in the Participant’s privacy practices;

   j) That collected information is subject to disclosure pursuant to judicial or other government subpoenas, warrants, orders, or if the Participant mergers with or is acquired by a Third Party, or goes bankrupt;

   k) Effective date of Privacy Statement;

   l) If required, statement of participation in the TRUSTe program and define participation scope; and
m) Information on how to contact TRUSTe to express concerns regarding Participant’s Privacy Statement or privacy practices.

2. At a minimum, Participant shall link to a Comprehensive Privacy Statement that discloses the Participant’s information practices.

3. Access to the Privacy Statement shall be Clear and Conspicuous.

4. As commercially reasonable, Privacy Statement should be available when the Individual engages with the Participant, such as through an application, Web site homepage or landing page.

5. As commercially reasonable, Privacy Statement should be available at the point where the Individual provides PII, or through a common footer.

6. Participant shall treat all collected information in accordance with the posted Privacy Statement in effect at the time of collection unless the Individual otherwise has given Express Consent.

7. Short Notice
   a) If Participant chooses, they may provide a Short Notice highlighting their information practices including but not limited to:
      (1) Summarize what information is collected by the Participant and how the Participant collects that information, either through active or passive means;
      (2) Summarize how Participant uses collected information;
      (3) Whether Participant shares PII with third parties, excluding Service Providers;
      (4) How the Individual can exercise choice and request access pursuant to these Program Requirements; and
      (5) How to contact the Participant including company name, email address or link to online form, and postal address.
   b) Access to the Short Notice shall be Clear and Conspicuous.
   c) Short Notice shall link to Comprehensive Privacy Statement.
      (1) Access to the Comprehensive Privacy Statement shall be Clear and Conspicuous.
   d) Any Short Notice shall be consistent with Comprehensive Privacy Statement.

8. Just in Time Notice
   a) If Participant chooses to provide Just in Time Notice, the Just in Time Notice shall describe key collection and use details regarding the Participant’s CEUD containing PII or PII collection and use practices that are relevant to the Individual at a particular time.
9. **Foreign Language Privacy Statement.**

a) If Participant seeks TRUSTe certification of a Privacy Statement in a language other than English, TRUSTe shall use commercially reasonable efforts to verify that Participant’s Foreign Language Privacy Statement is an accurate translation of Participant’s English language Privacy Statement.

b) Participant shall ensure that its privacy practices are the same, and that the Foreign Language Privacy Statement provides materially the same description of Participant’s privacy practices as Participant’s English Language Privacy Statement.

c) Participant must notify TRUSTe of any Material Changes to its Foreign Language Privacy Statement and submit changes to TRUSTe for review and approval.

E. **Data Governance**

1. Participant shall implement controls and processes to manage and protect CEUD or PII within its control including the ones listed in this Section IV.E.

   a) Such controls and processes shall be

   (1) Appropriate to the size of the Participant’s business; and

   (2) Appropriate to the level of sensitivity of the data collected and stored.

2. **Data Security**

   a) Participant must implement commercially reasonable procedures to protect CEUD or PII within its control from unauthorized access, use, alteration, disclosure, or distribution.

   b) Participant shall maintain and audit internal information technology systems within Participant’s control such as:

   (1) Regularly monitor and repair systems including servers and desktops for known vulnerabilities;

   (2) Limit access and use of CEUD, PII, or PII collected from someone other than the Individual to whom the PII pertains, to personnel with a legitimate business need where inappropriate access, use, or disclosure of such CEUD, PII, or PII collected from someone other than the Individual to whom the PII pertains could cause financial, physical, or reputational harm to the Individual;

   (3) Implement protection against phishing, spam, viruses, data loss, and malware; and
(4) Use reasonable encryption methods for transmission of information across wireless networks, and storage of information if the inappropriate use or disclosure of that information could cause financial, physical, or reputational harm to an individual.

c) Participant shall utilize encryption such as Secure Socket Layer for the transmission of information if the inappropriate use or disclosure of that information could cause financial, physical, or reputational harm to an individual.

d) Access to CEUD, PII or PII collected from someone other than the Individual to whom the PII pertains retained by Participant must be at least restricted by username and password if the inappropriate use or disclosure of that information could cause financial, physical, or reputational harm to an individual.

e) Privacy Statement shall state that security measures are in place to protect collected CEUD, PII, or PII collected from someone other than the Individual to whom the PII pertains.

3. Data Quality

a) Participant shall take commercially reasonable steps when collecting, creating, maintaining, using, disclosing or distributing CEUD or PII to assure that the information is sufficiently accurate, complete, relevant, and timely for the purposes for which such information is to be used.

b) If any information collected by the Participant about an Individual is disputed by that Individual and is found to be inaccurate, incomplete, or cannot be verified, Participant shall promptly delete or modify that item of information, as appropriate, based on the results of the investigation.

4. Data Retention

a) If a Participant receives and retains CEUD, PII, or PII collected from someone other than the Individual to whom the PII pertains, the Participant must limit its retention to no longer than commercially useful to carry out its business purpose, or legally required; and must disclose in their privacy statement the approximate timeframe they will retain that information.

b) Regardless of the time period of retention, so long as a Participant has CEUD, PII, or PII collected from someone other than the Individual to whom the PII pertains in its possession or control, the requirements included herein shall apply to such information.

c) If requested by the Individual upon termination of the relationship between theParticipant and the Individual or when there is no longer a legitimate business need for the Participant to retain the Individual’s CEUD or PII, the Participant shall take reasonable steps to return, delete, destroy, or arrange for the destruction of information received from the Individual.
5. Service Providers
   
a) Participant must take commercially reasonable steps to ensure that its Service Providers with whom it shares CEUD or PII either:
      
      (1) Abide by Participant’s privacy policies as reflected in Participant’s Privacy Statement; or
      
      (2) Abide by privacy policies that are substantially equivalent to Participant’s privacy policies as reflected in Participant’s Privacy Statement; and
      
      (3) Abide by the rights and obligations attached to the CEUD or PII by the Participant regarding the security, confidentiality, integrity, use, and disclosure of the CEUD or PII.

6. User Complaints and Feedback
   
a) Participant shall provide users with reasonable, appropriate, simple and effective means to submit complaints, express concerns, or provide feedback regarding Participant’s privacy practices.

b) Participant shall also cooperate with TRUSTe’s efforts to investigate and resolve non-frivolous privacy complaints, questions and concerns raised either by:
      
      (1) Users through TRUSTe’s dispute resolution process; or
      
      (2) TRUSTe.

7. Data Breach
   
a) Participant must notify an Individual of a data breach within 45-days of a known breach if required by law.

b) Participant, if legally required to notify Individuals of a data breach, must notify TRUSTe and provide a copy of the notice to be sent or sent to affected Individual(s).

F. Other Collection and Use of PII about Individuals
   
1. Participant shall use PII collected from someone other than the Individual to whom the PII pertains solely to facilitate the one-time completion of the transaction that is the Primary Purpose for which the Participant collected the information without the Individual’s consent.

2. Participant must obtain Express Consent from the Individual to whom such PII pertains before such PII may be used, disclosed, or distributed by the Participant for any purpose other than the Primary Purpose for which the Participant collected such information.

   a) Participant may use the PII collected to send a one-time message to the Individual to solicit their Express Consent.

3. Regarding PII collected from someone other than the Individual to the whom the PII pertains the Privacy Statement shall state:
a) The types of the entity(ies) collecting such PII;

b) What kind of PII is collected, either through active or passive means;

c) How collected such PII is used and/or disclosed;

d) What types of additional Third Parties if any, including Service Providers, collected such PII is shared with.

G. Collection and Use of Precise Geo-location Data obtained via Location Services

1. Participant must obtain Express Consent from the Individual the first time Geo-location Data is used by the Participant to provide services.

2. Participant may provide additional notifications through a Just in Time Notice or a persistent icon, to remind Individuals that their Geo-location Data is being used by the Participant to provide a service.

3. Participant must obtain Express Consent from the Individual prior to the sharing of Geo-location Data with Third Parties other than Service Providers.

4. Participant must obtain Express Consent from the Individual prior to any use of Geo-location Data for Secondary Purposes.

5. Privacy statement shall state:
   a) How Geo-location Data is used;
   b) If Geo-location Data is used to create a profile about the Individual;
   c) How long Geo-location Data is retained;
   d) What type of Third Parties, including Service Providers is Geo-location Data is shared with and for what purpose;
   e) How the Individual can restrict the disclosure of Geo-location data to Third Parties; and
   f) How the Individual can revoke consent to the Participant’s collection and use of Geo-Location Data.

   (1) Such mechanism shall be easy to use.