A MODEL PRIVACY POLICY FOR SMART GRID DATA
INSTITUTE FOR ENERGY AND THE ENVIRONMENT
VERMONT LAW SCHOOL

Introduction & Use of this Policy

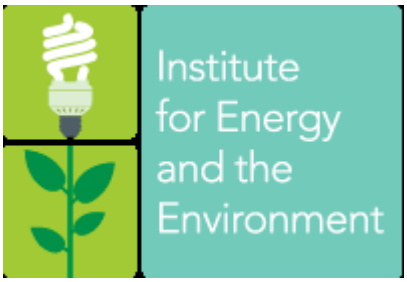
Advanced metering infrastructure and other emerging smart grid technologies have the potential to revolutionize the ways in which Utilities provide services to their Customers. Such technologies can:

- Improve reliable electric service
- Reduce Utility operating expenses
- Reduce Customer cost;
- Help Customers make informed choices that could reduce their electricity consumption.

One of the advances of the Smart Grid is that it enables the collection and reporting of individualized granular data about Customer electricity demand. Despite these manifest benefits, however, electric Customers have legitimate concerns regarding the manner in which such data is collected and how it is used. They want to preserve the privacy of their personal information.

The goals of implementing a more intelligent and responsive electric infrastructure and maintaining Customer privacy are not mutually exclusive. What is required is a policy or set of rules and procedures that govern how information is used and collected, and which prevents misuse or public disclosure. Such a policy will act as a roadmap for utilities responsibly to implement smart grid technology while providing their Customers with the assurance that concrete, identifiable safeguards are in place to protect personal information.

The authors hope that the following Model Privacy Policy will provide a foundation for Customer dialogue and a starting point for utilities to develop their own policy, adapted to the needs of their Customers and the regulatory environment of their jurisdiction(s).[1]



[1] The authors do not in any way warrant or present that this Model Policy is compliant with the laws of the jurisdiction in which the Utility operates. Before implementing any new rules or policies, the Utility should consult with legal counsel to ensure compliance with applicable, state, and federal laws and regulations.

TABLE OF CONTENTS

§ I. Statement of Policy

It shall be the policy of this Utility to preserve the privacy of Customer personal identifying information (PII), as defined in § II below, to the maximum extent possible. The Utility shall use all reasonable means to ensure that (1) only that PII which is reasonably necessary for the Utility to provide services to Customers is collected and retained, (2) that any PII collected is accessed only by those Utility Employees and Independent Contractors who have a legitimate business need connected to the provision of Utility services to Customers for such data, (3) that PII is not disseminated outside the Utility except to the extent necessary to provide Utility services to the Customers, (4) that prior written notification and, where possible, prior consent, be given to any Customer before his or her PII is released to a Third Party, (5) that Confidential Information, with or without PII, be kept confidential and released only to the extent necessary to provide Utility services, (6) that Confidential Information be made available to the Customers from whom such data was collected, or to that Customer's designee upon reasonable notice and request, and (7) that appropriate safeguards, including technological/cyber-security, employee screening, training and monitoring, and administrative procedures be implemented to protect the privacy of Customer information, including PII, to the maximum extent possible.

---

§ II. Definitions

A. Confidential Information: Confidential Information consists of the following three groups of data:

1. **Anonymous Personal Usage Information**: Anonymous personal usage data is any information that is collected, received, and/or stored by the Utility regarding the electrical demand and/or usage habits of individual Customers or small groups of Customers that, either explicitly or implicitly, reveals details, patterns, or other insights into the personal lives, characteristics, or activities of individual Customers or members of the group but which does not reveal the identity of the consumer or group from whom the information was collected.

   Such information shall not be considered anonymous if it contains PII or any other information from which a Third Party could reasonably deduce the identity of the Customer or Customers from whom such data is collected.

2. **Personally Identifiable Information ("PII"):** PII includes specific items of information that reveal, or reasonably could be expected to reveal the identity of an individual or small group of Utility Customers, including:
   i. Names
   ii. All geographic subdivisions smaller than a county, including street address, city, county, precinct, zip code, and their equivalent geo-codes;
   iii. All elements of dates directly related to an individual;
   iv. Telephone or fax numbers;
   v. Electronic mail addresses;
   vi. Social security numbers;

vii. Account numbers (including energy bill account numbers, credit card numbers, bank account numbers, etc.);
viii. Any information received in the credit check processes, and any unique personal identifying information related to finances;
ix. Certificate and license numbers;
x. Network/Internet Protocol address, LAN, and other unique digital networking information;
xi. Device Identifiers and serial numbers;
xii. Biometric identifiers, including finger and voice prints;
xiii. Photographic images and any comparable images that could identify an individual Customer;
xiv. Any other unique identifying number, characteristic, or code.

3. **Private Customer Information**: Any information that combines PII with Anonymous Personal Usage Information or which otherwise could allow individual Customer electricity usage data and/or behavioral habits to be attributed to an identifiable Customer or small group of Customers.

B. Non-Confidential Information: Confidential Information consists of the following two groups of data:

1. **Public Information:** Any non-privileged or non-Personally Identifiable Information prepared, owned, used, or retained by the Utility that is required or intended to be disclosed or made available to the public. This information may include general characteristics of the Utility's total load and generation mix as well as general information regarding rates and programs.

2. **Aggregate Use Data:** Aggregate Use Data refers to information regarding the usage habits of a sufficiently large group of utility Customers or broad categories of Customers (e.g. industrial business, residential) collected in a way so the person receiving such information is highly unlikely to deduce the identities and/or electricity usage habits of individual Customers within the group for which the information has been aggregated.

C. Third Parties

1. Vendors: An entity selling products or services to the Utility's Customers that does not directly provide services to the Utility in the Utility's ordinary course of business.

2. Independent Contractors: An entity or person performing a function or service under contract with or on behalf of the Utility, such as billing, Customer service, demand response, payroll services, or other functions related to providing reliable electric service.

D. Customer(s): Customer(s) means any person, corporation, government or other legal entity to which the Utility provides electricity and/or ancillary services or from whom the Utility

collects Confidential Information. For purposes of this Policy, "Customer" includes persons or entities that receive such services regardless of whether they have a contractual relationship with the Utility or pay compensation for the services received.

§ III. Customer Privacy & Other Rights

A. Collection of Customer Confidential Information

1. Before collecting any new confidential information from Customers or implementing any programs or systems that automatically collect Confidential Information, the Utility shall determine what Confidential Information is reasonably necessary to effectively implement Smart Grid Technology.
2. Consistent with cost considerations and available technology, the Utility shall endeavor to collect only that Confidential Information identified as reasonably necessary in subparagraph A(1) above.
3. Before the utility begins collecting any Confidential Information, the Utility shall make available to Customers a summary of the types of Confidential Information that will be collected and the reason(s). This summary shall be posted on the Utility's Internet site, updated at regular intervals to reflect changes in technology or Confidential Information collection practices, and made available to Customers upon request.

B. Customer Right of Access

1. Customers shall be entitled to access their own Private Customer Information within a reasonable time after the Utility collects and verifies the data. This information will be presented in an easily readable format that is as detailed as the information that the Utility uses in providing its services to the Customer. The Utility will make reasonable efforts to ensure that Customers have options regarding how they receive such information from the Utility, such as postal mail, electronic mail, utility website account, etc.

2. The Utility will provide Customers with access to their own Confidential Information through a convenient, user-friendly Internet website interface.

3. Customers shall have the right know what personal information the Utility maintains about the Customer. The Utility will make a reasonable effort to respond to requests for such information within five business days of being contacted by the Customer.

C. Customer Right to Accuracy

1. The Utility shall ensure that the information it collects, stores, uses, and discloses is reasonably accurate, and complete, and otherwise compliant with applicable rules and tariffs regarding the quality of energy usage data.

2. Customers shall have the opportunity to dispute the accuracy or completeness of Confidential Information, including Personally Identifiable Information that the Utility has collected for that Customer. The Utility will provide adequate procedures for Customers to

dispute the accuracy of their Confidential Information, and request appropriate corrections or amendments.

D. Customer Right to Privacy

1. Except as provided in Section IV of this Model Policy, the Utility shall not disclose any Confidential Information (including Anonymous Personal Usage Information, Personally Identifying Information or Private Customer Information) to any person or entity, including Utility Employees and Contractors.

E. Customer Right to Disclose Confidential Information

1. Notwithstanding any other provision of this Policy, Customers shall have the option to share their Confidential Information with Third Parties (e.g. service providers that facilitate compatible devices, technologies, and appliances that augment the visibility, understanding, and control of electricity consumption.) The Utility shall implement procedures for enabling Customers to share such information, including electronic copies of their Private Customer Information or through "click through" or "green button" technology.

2. Whenever a Customer requests access to their own Confidential Information, whether electronically or in writing, the Utility may require that the Customer agree that the Customer is solely responsible for the information that the Customer chooses to disclose any information that the Third Party thereafter makes of such information.

3. Whenever the Utility allows Customers to transfer information directly from the Utility to a Third Party through "click through" or "green button" technology, the Utility shall disclose to the Customer the specific elements of Confidential Information that are to be released in order to allow the Customer to make an informed decision prior to releasing such information to the Third Party.

F. Customer Right to Information Education

1. The Utility shall implement a continuing Customer education program. This program shall offer informational materials to Customers regarding Smart Grid technology, the ways in which Customer Confidential Information is being used, the procedures by which Confidential Information may be shared, and guidance for Customers to make informed and responsible decisions regarding sharing information with Third Parties.

2. The Privacy Officer designated by the Utility in accordance with § VI(A) of this Policy shall have primary responsibility for designing and overseeing the continuing Customer education program set forth in §III(F)(1) and shall have discretion in designing a program that is cost effective and tailored to the needs of the Utility's various Customer bases.

§ IV. Permitted Disclosure of Customer Information & Procedures

A. Disclosure to Utility Employees/Employee Access

1. The Utility will limit access by its Officers and Employees to Confidential Information so that each Employee or Contractor has access only to the information that is needed to perform their assigned duties.

2. Prior to granting Officers and Employees access to Confidential Information, the Utility shall ensure that the Officers and Employees satisfied all of the requirements of § V(B) These requirements may be satisfied either during a new Employee or Officer's hiring and orientation process or, in the case of an Officer or Employee whose previous duties did not involve access to Confidential Information, prior to being assigned new duties that do involve such access.

.

3. The Utility shall require Officers and Employees to surrender all Confidential Information, including duplicate or electronic copies, promptly upon their departure from Utility employment or reassignment to a position that does not require access to Confidential Information to perform regularly assigned duties. The Utility shall implement, and the Privacy Officer shall enforce, procedures sufficient to verify compliance with this paragraph.

B. Disclosure to Contractors and Venders

1. The Utility may share Confidential Information with Contractors and Venders only to the extent necessary for such Contractor or Vender to carry out services required by the Utility. Before sharing such information, the Utility shall determine what information/type of information is necessary for the Contractor or Vender to provide their service and limit disclosure to such information.

2. Before disclosing any Confidential Information to a Contractor or Vender, the Utility shall require the Contractor or Vender to certify in writing that they have read, understand, and will comply with all requirements of this Privacy Policy in the same manner as if they were Employees of the Utility. As a precondition to disclosure, all such Venders and Contractors shall sign a non-disclosure agreement stating that Utility Customers are intended third party beneficiaries of the non-disclosure agreement.

3. The Utility shall take the appropriate action, including taking appropriate legal action, in the event of breach of contract by any Third Party who violates any provision of the contract regarding Customer privacy.

4. The Utility shall require that all Contractors and Venders who seek access to Confidential Information have policies, procedures and technological safeguards in place sufficient to prevent the misuse and/or improper or unauthorized dissemination of Confidential Information. The Utility shall verify the existence and efficacy of such procedures before first releasing Confidential Information to the Contractor or Vender, and then at regular intervals thereafter.

C. Disclosure of Non-Confidential Information to Other Third Parties

1. When authorized, but not required by law, the Utility may disclose information, other than Confidential Information to government agencies, researchers, or other entities who request access to such Information. To the fullest extent allowable by law, the Utility shall ensure that only Non-confidential information is shared. Confidential Information may only be shared with informed, written consent of the Customer.

D. Disclosures Required By Law

1. To the fullest extent allowable by law, the Utility will comply with all obligations to provide Information, including Confidential Information in the following manner:

a. General Information/Freedom of Information Act ("FOIA") The Utility will only provide Non-Confidential Information in response to a request for Information made pursuant to a FOIA or analogous statute.

b. Customer Specific Confidential Information/Warrants: The Utility shall comply with requests for Confidential Information when such information is demanded through a valid legal process, such as through a warrant or subpoena. Upon receipt of a warrant, the Utility shall:

i. Notify the Customer(s) whose information has been demanded or requested and transmit a copy of the document containing the demand or request to the Customer(s) within three (3) days after first receiving it unless such notification is precluded by court order or other law.

ii. Cooperate with the Customer(s) in seeking an extension of time to respond to the demand or request so that the Customers(s) may assert their interests and rights.

iii. Nothing contained in § IV(E)(1)(b)(i) & (ii) shall preclude or in any way diminish the right of the Utility to object to, move to quash, oppose or seek qualifications such as a protective order to the demand or request.

E. Disclosure to Other Third Parties/Customer Consent Required

1. The Utility shall not disclose Confidential Information to a Third Party other than those enumerated in § IV(A),(B), (C) &(D) of this Policy without the prior informed, written consent of the Customer(s) from whom the Confidential Information was collected.

a. Form of consent: Customer informed, written consent shall be effective only if it is:

i. Given after a full disclosure of the material facts, specifically including the identity of the Third Party to which the information is disclosed, the use that Third Party intends to make of the Confidential Information, and any limits on the use and further disclosure of the Confidential Information imposed by the utility;

ii. Given in writing, including electronic approval, by the Customer; and

iii. Identifies by name the Third Parties to which it applies.

b. Consent Forms Prepared By the Utility: If the Utility uses its own form to obtain Customer consent, that form must be transmitted to the Customer separate from all other correspondence from the Utility, must specifically identify the name of the Third Party to whom the data will be disclosed, and must contain a statement advising the Customer of the right to revoke consent, and the procedures for so doing.

c. No inference of Consent from Silence: In no case shall silence by the Customer ever constitute express or implied consent to a request by the Utility or Third Party.

d. No penalty for Withholding Consent: The utility shall not withhold any service, or impose any other penalty on a Customer based in whole or in part on that Customer's failure or refusal to provide the Utility with written consent to share Confidential Information with Third Party Vendors.

e. Revocation: Subject to agreements with Third Parties, a Customer has the right to revoke, at any time, any previously granted authorization to transfer Confidential Information to a Third Party.

f. Upon receipt of revocation from a Customer, the Utility shall as soon as possible, but no longer than one full billing cycle, to cease further disclosure of that Customer's Confidential Information.

2. The Utility will be responsible for any breach of agreement with a Third Party that results from the Customer's decision to stop sharing Confidential Information with an authorized Third Party.

3. When a Customer is enrolled in a voluntary program where the Customer shares Confidential Information with the Utility, or its Contractors, or Vendors the Utility will contact the Customer once every calendar year to inform the Customer of the authorization granted and to provide an opportunity for revocation from Vendors.

---

§ V. Privacy Safeguards

A. Comprehensive Information Technology Security Systems

1. Prior to implementing any plan calling for the collection of Confidential Information, the Utility shall investigate options for deploying a Comprehensive Information Technology Security System ("CITSS"), which integrates hardware, software, and human resources at all points along the data lifecycle to prevent the misuse or disclosure of Confidential Information.

2. Following completion of the investigation required by § V(A)(1) and prior to the collection of any Confidential Information, the Utility shall select a CITSS that is secure according to industry practices and best practices for data storage.
    a. Provided that any system selected meets industry standards and best practices, the Utility shall have discretion in selecting a CITSS and may balance costs against incremental improvements in information security.
    b. In selecting and implementing a CITSS, the Utility shall consider implementing the following features:
        i. Systems that store Confidential Information separately from other information possessed by the Utility.
        ii. Systems that store Confidential Information offline so as to prevent outside security breaches.
        iii. Systems that compartmentalize and separate Confidential Information in such a way that breach of one system, or access to one system, will not give access to all Confidential Information (i.e., systems that segregate and firewall different types of confidential information, or which store Confidential Information from different regions separately).
        iv. Systems that employ a high level of encryption and require multiple-step authentication to access.
        v. Systems that can detect and respond to breaches rapidly.
        vi. Systems which are secure at all points in the data lifecycle, including at the point of collection on the Customer's premises.
        vii. Systems that securely dispose of, or securely transfer offline any Confidential Information no longer needed by the Utility to provide services.
        viii. Systems that incorporate any other features that either are considered standard in the industry, or which are recommended by the Utility's experts or consultants.

3. Following implementation of a CITSS, the Utility shall retain an independent consultant to test and make recommendations regarding the CITSS. The Utility shall correct any serious deficiencies in the CITSS identified by the consultant as at risk for unauthorized disclosure of Confidential Information, and shall consider any recommended, non-essential improvements.

B. Employee/Third Party Contractor Security

1. **Criminal Background Check:** Officers, Employees, and Contractors whose jobs require access to Confidential Information shall undergo a criminal background check before gaining access to such Confidential Information. Any prior misdemeanor or felony violation related to privacy or which involved dishonesty or moral turpitude shall disqualify that Officer, Employee, or Contractor from access. The utility shall have discretion to refuse to grant access to any person regardless of criminal background.

2. **Training and Procedures:** The Utility shall implement procedures and training protocols designed to maximize the security of Confidential Information at all points in

the data lifecycle, including data collection, storage, use, retention and disposal. The Utility shall also train all Employees and Contractors in these procedures prior to granting access to Confidential Information.

a. The Utility shall evaluate and update its privacy procedures and training materials at regular intervals to account for new technologies and developments. When such updates or changes are made, the Utility shall require Officers, Employees and Contractors who have been granted access to Confidential Information to update training with the changes as a condition to continued access.

b. The Utility shall implement a procedure for the prompt initiation of an investigation and, if appropriate, discipline, of any Officer, Employee, or Third Party who discloses Confidential Information to unauthorized persons or entities. The Utility's employee discipline policy shall allow the Utility to terminate any Officer, Employee or Third Party found to have intentionally or recklessly disclosed Confidential Information to unauthorized persons or entities. No provisions of this subsection shall preclude the Utility from handling negligent or inadvertent disclosures of Confidential Information through its existing employee discipline or performance review policies.

c. The Utility shall inform Officers, Employees and Third Parties of the severe consequences of unauthorized disclosure of Confidential Information during training.

3. **Nondisclosure Agreement**: Prior to earning access to any Confidential Information, all persons identified in §V(B)(1) shall be required to execute a non-disclosure agreement preventing that Officer, Employee, or Third Party from disclosing Customer Confidential Information without authorization.

---

§ VI. Controls and Audits

A. Privacy Officer

The Utility will identify an Officer or Employee responsible for implementing and reviewing Utility privacy procedures. This may require the creation of a new Officer position, or may be delegated to an existing Employee or Officer.

1. The Privacy Officer shall have primary responsibility for all aspects of Information Security, including:
   - **a**. Overseeing the implementation, maintenance and improvement of the CITSS, described in § V(A);
   - **b**. Drafting security and training protocols and ensuring enforcement;
   - **c**. Identifying Officers, Employees, and Third Parties subject to trainings and ensuring each are properly trained;
   - **d.** Ensuring surrender of Confidential Information by Officers, Employees and Contractors who no longer require access to such information;
   - **e**. Overseeing the secure destruction of obsolete or unnecessary Confidential Information;
   - **f**. Overseeing the Utility's response to any unauthorized access or use of

Confidential Information or breach of the systems in which such information is stored;

g. Overseeing audits or inspections of the CITSS as provided for by this Policy;

h. Performing any other duties deemed appropriate for this position as determined by the Utility.

2. The Privacy Officer shall report to the Utility's executive leadership or Board at periodic intervals not to exceed one year regarding the status of the Utility's privacy safeguards and CITSS and shall make recommendations and proposal regarding privacy improvement.

3. The Privacy Officer shall have overall responsibility for ensuring the timely provision of reasonably complete and accurate reports to Customers covering disclosures required by this Policy.

B. Privacy Impact Assessment (PIA) and Annual Review

1. Privacy Impact Assessment: The Utility shall complete a structured and reliable analysis of how the Utility handles information relating to or about individuals or groups of individuals. The assessment generates a report, similar to an audit report, describing the types of privacy risks discovered based upon each privacy category, documents the findings, and then provides recommendations for mitigating the privacy risk findings. Goals of the PIA include:

a. Determining whether the Utility's information handling and use complies with legal, regulatory, and policy requirements regarding privacy;

b. Determining the risks and effects of collecting, maintaining, and disseminating information in identifiable or clear text form in an electronic information system or groups of systems; and

c. Examining and evaluating the protections and alternative processes for handling information to mitigate the identified potential privacy risks.

2. Annual Review: The Privacy Officer shall undertake an annual review of the Utility's information collection, storage, disclosure, and destruction procedures. The annual review will also take into account developments or advancements in security technology or practices. Copies of the PIA and annual review shall be presented to the Utility's executive leadership or Board and, after being edited to remove any information that could enable unauthorized access to or use of Confidential Information, shall be made available to Customers upon request.

C. Independent Audit

1. The Utility will establish a procedure for a bi-annual independent audit of its information collection, storage, disclosure, and destruction practices. The Utility requires Third Parties with access to Confidential Information participate in the

independent audit or follow similar, adequate, procedures for independent auditing of security practices.

2. Notwithstanding the provisions of § VI(C)(1), in the event of a breach of the Utility's CITSS or other unauthorized access to or disclosure of Confidential Information, the Utility shall within two weeks after discovering that a breach or unauthorized access/use has occurred, cause an independent audit to be conducted into the cause of the breach or unauthorized access/use and take corrective measures based on the conclusions of that audit.

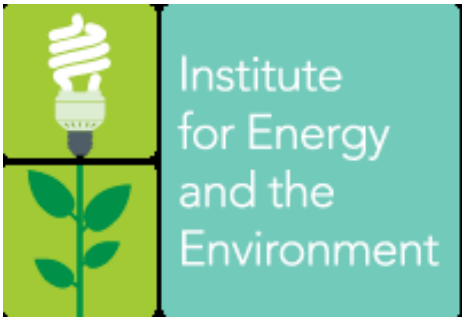
D. Mitigation and Customer Notification in the Event of Breach

1. As soon as practicable, but no longer than within one week after discovering a breach or unauthorized access/use of Confidential Information, the Utility shall notify all of its Customers of the breach and any information that may have been compromised or disclosed as a result thereof. The Utility shall provide regular updates to its Customers regarding the status of mitigation efforts, including data recovery efforts and system strengthening until the problems causing the breach have been identified and remedied.

2. In the event of a breach of the CITSS, or unauthorized access to or disclosure of Confidential Information, the Utility shall take all reasonable measures, including cooperating fully with law enforcement agencies, to recover lost information and prevent the loss of further Confidential Information.

Find this Privacy Policy published at: www.VermontLaw.edu/SmartGrid

Institute for Energy and the Environment at
Vermont Law School
www.VermontLaw.edu/Energy



AUTHORS

KATIE R. THOMAS, CHRISTOPHER D. SUPINO, COLIN R. HAGAN, KEVIN B. JONES

ACKNOWLEDGEMENTS

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000446.

The authors gratefully acknowledge the support of the staff of the Institute for Energy and the Environment, especially Jennifer Thomas, and the faculty of Vermont Law School, whose continuing support of this work made it possible.