Data Privacy Guidelines for Large Utilities

Contents

1. Overview

This document is intended to provide a guide to Public Utility Districts in developing a policy to address the specific obligations of utilities under RCW 19.29A and other applicable Washington laws, rules, and regulations regarding the collection use, disclosure, and protection of personally identifying information of the utility's customers. Utilities should consult with their local counsel before adopting the policies and procedures outlined in this document, as they may need to be modified and tailored as appropriate to address individual policies and practices.

Strong consumer data privacy protections are essential to maintaining the trust of our customers. We understand the importance of protecting the personal information we collect from the public. This document is intended to help utilities emphasize their commitment to protect customer data from unauthorized disclosure or breach of security throughout the lifecycle of the data. It will also help utilities understand some of the requirements imposed by RCW's related to data security, and will recommend some best practices utilities can follow to add levels of security above and beyond the minimum state requirements.

More and more customer information is being collected by utilities and is used to perform essential business functions such as operating and maintaining the system, managing outages, processing customer bills, credit and collections, conservation and usage management, etc. With the implementation of automated metering, even more detailed customer data is now being collected. Utilities must be committed to protecting the security and privacy of all customer data, and to conform to applicable laws and regulations, to keep this information private and secure.

This document is divided into several sections:

- Section 2 includes data privacy requirements for consumer owned utilities that must be incorporated in a policy approved by the governing board. To be in compliance with statute, the governing board must approve the policy by October, 2016.
- Section 3 addresses utility obligations when a breach of customer personal information has occurred. The breach can occur at the utility, or at with a subcontractor that has customer information.
- Section 4 includes information that may not be required by statute but should be considered as a utility develops internal policies and practices, and customer-facing documents, related to customer data privacy.
- Section 5 discusses the impacts of the Public Records Act on public entities, and considerations related to the release of information to law enforcement as allowed by statute.
- Section 6 includes information about contract management best practices. This section also addresses the statute requirement regarding utilities who utilize contractors to perform essential business functions, and, requirements regarding contracts when the contractor subcontracts to third parties to perform these functions. In this case, the statute requires that all contracts - with the primary contractor or with the subcontractor- include language that prohibits the release of customer information. This requirement must also be incorporated into the overall policy adopted by the governing board.
- An Addendum section includes examples of internal and external policies and documents that utilities can use as resources when drafting their own policies.

2. RCW 19.29A Consumers of Electricity - Utility Requirements

RCW19.29A establishes a number of requirements enacted by the Legislature that utilities must follow. During the 2015 legislative session, several new requirements were added to this chapter following the adoption of House Bill 1896 and House Bill 2264. Specifically, RCW 19.29A.100 and RCW 19.29A.110 were added as new sub-chapters, reflecting the requirements of the two house bills. Further, RCW 19.29A.100 (10) adds a due date for incorporation of the requirements into policy, which must be adopted by governing boards by October 9, 2016.

A summary of the requirements is as follows. A customer facing document that incorporates these requirements and can be approved by a board is provided as Addendum 1, and an internal policy with the requirements is in Addendum 2:

2.1 Customer Consent to Release Data

In accordance with RCW 19.29A.100 a utility may not sell private or proprietary customer information. Further, the utility cannot disclose private or proprietary information for the purposes of marketing services or product offerings the customer does not already subscribe to. In order to disclose information to a third party for this purpose, a utility first must obtain a customer's permission prior to releasing the information. The RCW defines proprietary and private customer information as a customer's name, address, telephone number, and other personally identifying information, as well as a customer's usage, payment history, and other information the utility has solely by virtue of the utility-customer relationship.

Customer consent is *not* required when the utility releases private and proprietary information when performing an essential business function, i.e. to a third party vendor. Therefore it is recommended that a utility define the purposes that customer data will be used when released to a third party. As an example, the utility should distinguish the release of data for *primary* purposes, such as generating a bill, printing and mailing a customer newsletter, or energy efficiency program administration data. The utility should also define data used for a *secondary* purpose such as marketing services or products. A sample definition is as follows:

Primary Purpose - data released for essential business functions, such as billing or bill presentment, energy efficiency program validation or administration (such as BPA), and customer surveys. When data is released to a vendor to provide services that are of a primary purpose, the vendor is further prohibited from disclosing the customer information to a party that is not under contract with the utility or its contracted affiliates. Further, the vendor must sign a Confidentiality and Non-Disclosure Agreement.

Secondary Purpose - data released for marketing services or product offerings the customer does not already subscribe to. Requests for customer data used for secondary purposes might come from a customer asking for their data to be shared directly to a third

party vendor, from a vendor asking for customer information for marketing purposes, or from utility staff working with a third party to market a new product or service.

Obtaining Affirmative Customer Consent - Release of Data for a Secondary Purpose
When data is released for a secondary purpose, affirmative (advance) consent must be obtained from the customer prior to the release to the third party. In accordance with the RCW, the utility must, in part:

- Maintain a record for each instance of consent
- Provide the ability to receive consent via hard copy or electronically.
- Confirm that the customer providing the consent exactly matches the utility record for that customer.
- Provide the customer with an option to withdraw the consent.
- Refer to RCW 19.29A.100 for the complete list of requirements.

A sample Customer authorization to Release Information is included as Addendum 5.

Affirmative customer consent is not required in the following circumstances

- When the data is aggregated. Refer to the definitions section for the definition of aggregated data.
- When the data is disclosed to effect, administer or complete a financial transaction that the electric customer requested or otherwise authorized; however, the data cannot be further disclosed (i.e. for marketing purposes).

2.2 Release of Data to a Person

RCW 19.29A.110 addresses the release of customer information to a "Person," with Person being defined as any individual, partnership, corporation, LLC or other organization or commercial entity except an electric utility. Persons who request non-exemptible customer information must first obtain consent from the customer before receiving said information, if the data will be used for commercial or marketing purposes. However, consent is not required if the customer initiated the purpose of the release (for example, a realtor requests usage information on behalf of a customer for a house they are selling).

While utilities are not expected to be enforcers of this RCW sub-chapter, it is something to be aware of. It is recommended that utilities make the recipient aware of the requirements established by this RCW, i.e. the data cannot be used for commercial or marketing purposes unless the customer has given consent to the Person to do so. A sample Usage History Report that a utility would provide to a Person requesting usage information is included as Addendum 9. This sample includes disclaimer language regarding the recipient's use of the data.

2.3 Resolution of Customer Complaints – Disclosure of Data

In accordance with RCW 19.29A.100, utilities are required to establish a policy that must include procedures for investigation and resolution of complaints by a customer whose private or proprietary information may have been sold or disclosed by the utility for the purposes of marketing services or products.

A sample "Complaint Investigation Process" is provided as Addendum 6 that describes the actions a customer must take to request an investigation if they suspect that their information has been released, and the steps the utility must take in response.

2.4 Contractor/Third Party Contract Requirements

While utilities can release customer data to vendors for primary business purposes, RCW 19.29A.100(5)(a) requires the contract with that vendor contain language preventing the vendor from further disclosing or selling any provide customer information.

A sample Confidentiality and Non-Disclosure Agreement (CNDA) that meets this requirement is provided as Addendum 4.

3. Required Notification – Data Breaches

Under RCW 42.56.590, when a breach of personal data occurs, utilities are required to disclose the breach to the customers whose data was acquired by an unauthorized person. This notice needs to be provided as soon as the utility discovers the breach or is notified of the breach (for example, from a third party vendor who has personal information for a primary or secondary business purpose), subject to the following:

- Notice is not required if the breach is not likely to subject the customer to a risk of harm.
- Required notification may be delayed if a law enforcement agency will impede a criminal investigation.
- The notice can be written or electronic.
- Depending on the cost of the notification, other options exist to provide this notification.

Utilities should refer to the RCW for additional requirements regarding breaches.

Contractor Responsibility
It is recommended that utilities include language in their contracts that contractors provide timely notification of a breach to the utility. Please refer to the Confidentiality and Nondisclosure Agreement (Addendum 4) for sample contractor responsibility language.

4. Other Considerations – Model Data Privacy Policy

While not required by law, utilities should consider creating an internal policy that addresses different aspects of customer data privacy and sets the standards the utility will follow to protect customer data. When developing a data privacy policy, utilities should consider including the following (see sample internal policy provided as Addendum 2). This sample policy incorporates the following topics:

4.1 Aggregated Data

Customer consent is not required when releasing aggregated data. In accordance with RCW 19.29A.100 (8), aggregated data is data that is considered sufficiently consolidated so that any individual customer cannot reasonably be identified. Utilities may want to establish their own definition of aggregated data to include in their policy. APPA has developed a 15/15 rule which achieves this level of consolidation. The 15/15 rule states that aggregated data must include the data of at least 15 customers, and that no single customer included in the sample is to comprise more than 15% of the total aggregated load. Any personally identifying information must be removed from the aggregated data before release.

4.2 Personally Identifiable Information (PII)

Each utility may want to define Personally Identifiable Customer Information, or PII, to incorporate into their policy. The utility definition of PII may be more restrictive than what is established by local, state and federal laws. A sample definition of PII is as follows:

1. Names
2. Street addresses
3. Telephone numbers
4. Email addresses
5. Social Security numbers
6. Account numbers (including utility account numbers, credit card numbers, bank account numbers)
7. Account balances
8. Any information received to identify the customer, such as driver's license, passport, or information collected to establish their credit worthiness.
9. Meter identifier and meter interval/electricity use data that is released ***in combination with*** any information included with items # 1-8 above.

RCW 19.29A.010 (25) and (26) also provide definitions for Private Customer Information and Proprietary Customer Information.

4.3 Transmittal of PII

It is considered a cyber security best practice to send customer data and PII to external parties using FTP or encrypted websites. While email and hard copies are often times the easiest forms of transmittal, keep in mind that email can be intercepted and hard copies can be misplaced or lost through the mail.

4.4 Transmittal of PII over Advanced metering infrastructure (AMI)

Utilities with AMI systems need to be aware of the data that is being transmitted over their networks and if it contains PII. If it contains PII, efforts should be taken to ensure the network is secure and customer data cannot be accessed or obtained if the network is breached.

5. Public Records Requests

Public utilities must comply with RCW 42.56, the Public Records Act. Within the PRA, exemptions exist that prevent the release of certain personal information. The Summary of Disclosure of Customer Data (Addendum 8) summarizes the types of information a utility might be asked to release via a public records request, and if exemptions exist that prevent the release of the data. Public Records Requests can be submitted by Law Enforcement, or from the general public.

5.1 Disclosure of PII/Customer Information to Law Enforcement

RCW 42.56.335 gives law enforcement authorities a mechanism to obtain records of individuals who are suspected of committing a crime. The law enforcement officer must provide the utility with a written request that states the authority suspects the individual to whom the records pertain is suspected of committing a crime, and the authority believes the records could help determine if the suspicion is true.

A sample law enforcement request form "Request for Inspection, Copying or Obtaining of Public Records by Law Enforcement Agencies" is provided as Addendum 7.

Customer information that is strictly protected from disclosure by law will not be released to law enforcement under the above process. In order for law enforcement to obtain exemptible data, a subpoena, warrant or other form of court order must be obtained by the requesting agency.

6. Contracts Best Practices and Statute Requirements

Utilities may engage a contractor to provide services in support of primary and secondary business functions as noted above without obtaining advance customer consent. As noted above in Section 2.4, a Confidentiality and Non-Disclosure Agreement (CNDA) must be included as part of the standard contract language and approved as part of the utilities standard contract approval process. Further, the contractors may engage a subcontractor or third party to provide services in support of their contract with the utility. In accordance with the statute, a CNDA must be signed by a subcontractor or third party, ensuring the subcontract or third party will not sell or release PII for marketing or commercial purposes. A sample CNDA is provided as Addendum 4.

Utilities that assign an internal Contract Work Manager (CWM) to manage contracts throughout their life cycle should also ensure the CWM is aware of their obligations as it relates to the protection of customer data and it's release to a third party. A sample "Non-Disclosure Agreement Checklist" is provided as Addendum 3 to create that awareness as the CWM is preparing the contract.

Releasing Information to Contractors – Method it is released
It is recommended that the transmittal of files and forms that include PII to Contractor/subcontractor be sent via secure FTP or encrypted in order for a vendor to conduct business of the utility. Email or hard copies should never be used to share PII with a vendor.

7. Addendum

Addendum 1: Sample Customer Rights Statement/Customer Data & Privacy (Customer Facing)

This Customer Rights Statement shares our guiding principles for how we operate and conduct our business related to the security, privacy, and use of customer date, and matters of customer choice. Consumer trust is essential to the success of new technologies, and protecting the privacy of customer data is one crucial component of strengthening this trust.

[Utility] collects and uses customer data to perform essential business operations such as operating and maintaining the system, managing outages and processing customer bills. In using this data, **[Utility]** will conform to applicable laws and regulations intended to keep this information private and secure. Moreover, **[Utility]** recognizes its responsibilities may appropriately extend beyond these laws and regulations and as such has developed this Customer Rights Statement.

[Utility] customers have the right to:

- Privacy
    - We only share customer information with third parties in order to conduct essential business functions (such as bill processing services). We will not sell our customer's information. Our vendors are held accountable to the same standards regarding customer information shared with them.
    - We will obtain customer permission in advance of providing data to a third party for services the customer does not already subscribe to.
    - We only share customer information with the public in compliance with local, state, and federal laws. As a public entity, we will seek to protect the privacy of our customers' personal information in complying with public records requests.
    - We are committed to a fair resolution of privacy concerns. We provide our customers with an appeal process that allows them to voice concerns regarding the release of their information.
- Data Security & Integrity
    - We only capture data required to conduct our business and retain it for only as long as required.
    - We design security into every data collection, access and transfer point.
    - We will not transmit personally identifiable information over our Advanced Metering Infrastructure network.
    - We implement measures to protect against a loss, misuse, and alteration of the information we control.
    - We ensure delivery of an accurate bill and/or timely response if an error is discovered.
    - We will notify customers if any personal information is breached.

- Transparency
    - We conduct business in an open, transparent manner where our privacy policies and decisions are available to the public.
    - We provide information to our customers about all aspects of their account. The District will strive to provide more accessibility for customers through the development of a web portal.

- Customer Choice
    - The District does not currently have a time-of-use pricing program in place. In the event a time-of-use pricing program is considered, development of such a program will be conducted through an open, public process.
    - We will not implement a Home Area Network that enables customers to monitor and control their own appliances without prior written consent.
    - We are confident in the advanced meter technology that we have deployed: however customers may opt-out of our advanced meters. Fees are established to offset the cost of meter replacement and manual reads.

Addendum 2: Sample Internal Policy (Internal Document that encompasses RCW requirements and best practices)

Customer Privacy Policy

Introduction

Strong consumer data privacy protections are essential to maintaining the trust of our customers. This Directive is intended to emphasize the District's commitment to protect customer data from unauthorized disclosure or breach of security throughout the lifecycle of the data.

Customer information [Personally Identifiable Information (PII) as defined below] is collected and used to perform essential business functions such as operating and maintaining the system, managing outages, processing customer bills, credit and collections, conservation and usage management, etc. With the implementation of automated metering, even more detailed customer data is now being collected. The District is committed to protecting the security and privacy of all customer data, and will conform to applicable laws and regulations, as well as internal standards and policies which are intended to keep this information private and secure.

The District may be required to release various types of customer information in response to a public records request, court order, search warrant or discovery request. When one of these events occurs, efforts will be made as allowed by law to notify customers of such requests before the information is disclosed.

Scope

This Directive applies to all District employees, Commissioners, and contract personnel with access to the District's systems and data, hereinafter referred to within this policy as "employees."

Personally Identifiable Information (PII)

The District is committed to the protection of Personally Identifiable Information (PII) to prevent its unauthorized use or disclosure. To this end, customer data defined as PII by this Directive is more restrictive than what is established by local, state and federal laws. Information considered PII covered by this Directive is limited to:

1. Names
2. Street addresses
3. Telephone numbers
4. Email addresses
5. Social Security or Unified Business Identifier (UBI) numbers
6. Account numbers (Named Utility account numbers, credit card numbers, bank account numbers)
7. Account balances
8. Any information received during the identity and customer credit worthiness process
9. Identity information provided on a driver's license, passport, etc.
10. Meter interval/electricity use data that can be tied to items # 1-8 above.

Definition for the Use and Release of PII – Primary vs. Secondary Purpose

When customer data is released to a contractor/subcontractor or third party, the purpose of the release of the data will be defined as being for either a "Primary" or "Secondary" purpose, as follows:

Primary Purpose - data released for essential business functions, such as billing or bill presentment, energy efficiency program validation or administration (such as BPA), and customer surveys. When data is released to a vendor to provide services that are of a primary purpose, the vendor is further prohibited from disclosing the customer information to a party that is not under contract with the District or its contracted affiliates. Further, the vendor must sign a Confidentiality and Non-Disclosure Agreement.

Secondary Purpose - data released for marketing services or product offerings the customer does not already subscribe to. Data released for a secondary purpose requires affirmative customer consent (see definition below). Requests for customer data used for secondary purposes might come from a customer asking for their data to be shared directly to a third party vendor, from a vendor asking for customer information for marketing purposes, or from District staff working with a third party to market a new product or service.

Affirmative Customer Consent – Release of Data for Secondary Purpose

When releasing customer data for a secondary purpose, affirmative (advance) customer consent must be obtained for each instance of release of data unless the customer has previously provided advance consent.

The following is necessary to meet the requirements of affirmative consent, which can be provided electronically or via hard copy:

- The consent must include the date or date period for which the consent is granted.
- The consent must specify the party or parties the customer has authorized the release of their data to, including any affiliates and third parties.
- The District must validate that the individual providing the consent matches the name, service address and account number of the customer of record in the District's customer information system.
- A record for each instance the customer has given written or electronic consent must be maintained, following applicable records retention guidelines.

The attached "Customer Authorization to Release Information" (CARI) is provided as a template to use to obtain consent from a customer. CARI's obtained for a contract will be routed with the Contract Recommendation memo and CARI's obtained for customer-requested releases of their data will be retained in Customer Service.

Customers who have given affirmative consent also have the right to retract said consent at any time.

Aggregated Data

Aggregated data is data that is considered sufficiently consolidated so that any individual customer cannot reasonably be identified. The District will generally follow a 15/15 rule, which means that aggregated data must include the data of at least 15 customers, and that no single customer included in the sample is to comprise more than 15% of the total aggregated load. Any personal identifying information must be removed from the aggregated data before release.

Customer consent is not required when releasing aggregated data that meets this definition.

Disclosure of PII to Contractors/Subcontractors

As an electric utility, the District may engage a contractor to provide services in support of primary and secondary business functions as noted above. For new contracts, a Confidentiality and Non-Disclosure Agreement (CNDA) will be included as part of the standard contract language and approved as part of the standard contract approval process. Further, the District's contractors may engage a subcontractor or third party to provide services in support of their contract with the District. A CNDA must be signed by a subcontractor or third party and be routed through the normal contract approval process, accompanying the contract recommendation memo.

Responsibilities of Contract Work Manager - Release of PII for Primary Purpose

The Contract Work Manager (CWM) must review any need or request for PII to determine if PII shared with the contractor/subcontractor is necessary to meet the business objective.

- Any need or request to release PII to a contractor requires approval from the Assistant General Manager and Chief Privacy Officer. An approval only needs to be obtained the first time the District releases PII to that entity. Subsequent requests are only required if additional types of PII will be provided to the contractor.
- It is up to the CWM to reduce the amount of PII that is being released, where possible, by questioning the purpose and needs of the contractor to receive all information they are requesting.
- The contractor/subcontractor must provide a specific timeline in which the PII will be used and a scope that defines the manner in which the data will be used. Further, the contractor must comply with contract requirements that will address the disposition of PII after the contract timeline has expired.
- The CWM is also responsible for communicating the terms of the agreement to the contractor.

To facilitate this review, the CWM must complete the Non-Disclosure Agreement Checklist (below) and route it through the standard contract approval process.

Responsibilities of Contract Work Manager – Release of PII for Secondary Purpose

The CWM must obtain completed CARI forms from each customer whose data will be shared. Copies of the forms must be routed through the standard contract approval process.

The third party vendor the CWM is working with will be required to sign a CNDA.

Transmittal of PII to Contractor/Subcontractor

All files and forms of data provided to a vendor to conduct business of the District must be sent via secure FTP or be encrypted. Email or hard copies should never be used to share PII with a vendor.

Disclosure of PII During Customer Transactions

[Utility] considers security of PII a top priority, and will only share PII when requested with the customer(s) of record or an individual designated by the customer(s) of record to receive such information. Before releasing PII, measures will be taken to verify the identity of the person requesting the information. This may include asking for the UBI number of a commercial business, some combination of a social security number (first three digits, last four digits), or verification by driver's license number.

Disclosure of PII to Law Enforcement

The District will comply with RCW 42.56.235, which gives law enforcement authorities a mechanism to obtain records of individuals who are suspected of committing a crime. The law enforcement officer must complete a "Request for Inspection, Copying or Obtaining of Public Records by Law Enforcement Agencies" form before certain PII will be released to the requesting officer.

Customer information that is strictly protected from disclosure by law will not be released to law enforcement under the above process. In order for law enforcement to obtain this type of exemptible data, a subpoena, warrant or other form of court order must be obtained by the requesting agency.

All requests for PII by law enforcement should be processed through the District's Public Records Officer.

Breach Notice Practice

The District will implement administrative, technical, and physical safeguards to protect PII from unauthorized access, destruction, use, modification or disclosure.

If the District should discover or be informed of a breach, it will make an effort to secure the breached data and will ensure notification to all affected customers of the breach. The District will keep customers informed about the status of their information security as updates are made.

Addendum 3: Contract Work Manager Non-Disclosure Agreement Checklist (Internal Facing)

Non-Disclosure Agreement Checklist
(Routed with Contract Recommendation Memo)

It is the utilities policy to implement strong consumer data privacy protections to maintain the trust of our customers. The sharing of District customer, employee, or vendor information with third parties should occur only when it for a primary purpose and is necessary in the conduct of essential business functions.

Any Contract Work Manager (CWM) who requests that such information be shared with a third party will complete this checklist, sign, and route with the Contract Recommendation Memo.

The CWM's signature indicates that he/she is aware of the District's policy concerning Customer Privacy and in particular Personally Identifiable Information (PII) as defined in the policy. The CWM should evaluate the purpose of the information data sharing request and attempt to limit the amount of PII shared with the third party to that which is minimally necessary to meet the business objective.

The following customer/vendor/employee information will be shared with <Vendor Name> (check all that apply):

11. _____ Names
12. _____ Street addresses
13. _____ Telephone numbers
14. _____ Email addresses
15. _____ Social Security or Unified Business Identifier (UBI) numbers
16. _____ Account numbers (Named Utility account numbers, credit card numbers, bank account numbers)
17. _____ Account balances
18. _____ Any information received during the identity and customer credit worthiness process
19. _____ Identity information provided on a driver's license, passport, etc.
20. _____ Meter interval/electricity use data that can be tied to items # 1-8 above.

I have reviewed the information and data sharing request and believe that the PII identified above is that which is minimally necessary to accomplish the business objective, and that the data is being used for a primary purpose. A non-disclosure agreement is required with the contract.

By_____/_____
Contract Work Manager/Date

Title_____

Chief Privacy Officer: _____/_____
Date

Assistant General Manager: _____/_____
Date

Addendum 4: Confidentiality and Nondisclosure Agreement (Internal/Vendor Facing)

CONFIDENTIALITY AND NONDISCLOSURE AGREEMENT
Contract #XX-XX-XX

Date: _____

This Confidentiality Agreement ("Agreement") is by and between **[Utility]** a municipal corporation governed under RCW 54 of the laws of the State of Washington, and _____ ("Contractor").

For purposes of this Agreement, "Confidential Information" shall include **[Utility]** customer, employee, or vendor information, all technical and business information or material that has or could have commercial value or other interest in the business or prospective business of **[Utility]**, and all information and material provided by the **[Utility]** which is not an open public record subject to disclosure under the Washington Public Records Act. Confidential Information also includes all information of which unauthorized disclosure could be detrimental to the interests of **[Utility]** or its customers, whether or not such information is identified as Confidential Information.

For purposes of this Agreement, "Contractor" shall include all employees, consultants, advisors and subcontractors of Contractor ("its Representatives").

Contractor hereby agrees as follows:

1. Contractor and its Representatives shall use the Confidential Information solely for the purposes directly related to the business set forth in Contractor's agreement with **[Utility]** and shall not in any way use the Confidential Information to the detriment of **[Utility]**. Nothing in this Agreement shall be construed as granting any rights to Contractor, by license or otherwise, to any **[Utility]** Confidential Information.

Contractor agrees to obtain and utilize such Confidential Information provided by **[Utility]** solely for the purposes described above, and to otherwise hold such information confidential pursuant to the terms of this Agreement.

2. In the event third parties attempt to obtain the Confidential Information by legal process, the Contractor agrees that it will not release or disclose any Confidential Information until **[Utility]** has notice of the legal process and has been given reasonable opportunity to contest such release of information and/or to assert the confidentiality privilege.

3. Upon demand by **[Utility]**, all information, including written notes, photographs, memoranda, or notes taken by Contractor that is Confidential Information shall be returned to **[Utility]**.

4. Confidential Information shall not be disclosed to any third party without prior written consent of **[Utility]**.

5. It is understood that Contractor shall have no obligation with respect to any information known by it or generally known within the industry prior to the date of this Agreement, or become common knowledge with the industry thereafter.

6. Contractor acknowledges that any disclosure of Confidential Information will cause irreparable harm to the **[Utility]**, and agrees to exercise the highest degree of care in safeguarding Confidential Information against loss, theft, or other inadvertent disclosure and agrees generally to take all steps necessary to ensure the maintenance of confidentiality including obligating any of its Representatives who receive Confidential Information to covenants of confidentiality.

7. The obligation set forth in this Agreement will continue for as long as Contractor possesses Confidential Information. If Contractor fails to abide by this Agreement, the **[Utility]** will be entitled to specific performance, including immediate issuance of a temporary restraining order or preliminary injunction enforcing this Agreement, and to judgment for damages caused by the Contractor's breach, and to any other remedies provided by applicable law. Any breach of this Agreement shall constitute a default in performance by Contractor in any contract between the **[Utility]** and Contractor. If any suit or action is filed by **[Utility]** to enforce this Agreement, or otherwise with respect to the subject matter of this Agreement, the prevailing party shall be entitled to recover reasonable attorney fees incurred in the preparation or in prosecution or defense of such suit or action as affixed by the trial court, and if any appeal is taken from the decision of the trial court, reasonable attorney fees as affixed by the appellate court. This Agreement shall be governed by and construed in accordance with the laws of the State of Washington.

_____ Dated: _____

[Utility]

_____ Dated: _____

Consultant

Addendum 5: Customer Authorization to Release Information (Customer Facing)

CUSTOMER AUTHORIZATION TO RELEASE INFORMATION

This form is to permit [Utility) to release customer data as indicated below to a third party. The customer must complete this document in its entirety and must also be listed as a customer of record in **[Utility]** Customer Information System in order to authorize the release of said data.

Customer Information:

Account Number: _____

Name on Account: _____

Service Address: _____

Phone Number: _____

Email Address: _____ (if applicable)

I authorize the release of my customer data as follows:

Type of data to be released (i.e. usage or payment history, payment etc.) and the period in which the data covers (i.e. from January, 2014 through December, 2014 :

_____

_____

_____

Name of Recipient/Business: _____

Address: _____

Phone Number: _____

Manner in which data should be provided (mail, email, pick up): _____

Date(s) in which this release is in effect: _____

This data release is at the request of, and on behalf of the **[Utility]** customer listed above, and as such, the customer agrees to release and hold harmless **[Utility]** from any liability, claims, demands, causes of action, damages or expenses resulting from: 1) any release of information to the recipient noted above; 2) the unauthorized use of this information or data; and 3) from any actions taken by the recipient with respect to such information or data.

Account Holder Signature:_____ Date: _____

Addendum 6: Complaint Investigation Process (Customer Facing)

Complaint Investigation Process A customer has the right to request their utility investigate the potential release of their information.

A Customer shall utilize the following steps to initiate the investigation process

1. The utility must receive a customer's written request by personal delivery or mail, and shall be addressed to the (Named Utility).
2. The request must contain a short, plain statement of potential data released, the action requested by the customer and the appropriate customer contact information for purposes of communications for the appeals process.
3. Upon receipt of the request, the customer will be contacted by the utility's designee(s) within ___ business days and an informal conference will be scheduled.
4. The utility's designee(s) will investigate and will report back their findings of the investigation to the customer.
5. If the investigation is resolved to the satisfaction of the customer, the process is concluded.
6. If the situation remains unresolved, the customer may appeal the results of the investigation to (the governing board/general manager/hearing officer as designated by the utility's policy).

Addendum 7: Sample Law Enforcement Request Form (Internal)

REQUEST FOR INSPECTION, COPYING OR OBTAINING PUBLIC RECORDS BY LAW ENFORCEMENT AGENCIES

[Utility] *is governed by Title 54 of the Revised Code of Washington, and is subject to Washington state laws pertaining to the release of public records.*

This document is provided to allow law enforcement agencies to obtain disclosure of public records in accordance with [Utility Resolution Number]and the Washington Public Records Act. Authorized law enforcement representatives are required to provide proper identification and sign this form acknowledging the records being requested are being obtained pursuant to the requirements of the Washington Public Records Act.

For further information, please contact [contact info]

Date of Request: _____

Requestor's Name: _____
Representing Agency: _____
Identification provided: _____

Specific Document/Information requested:
_____
_____
_____
_____

Legal Process Requirements: The following types of records, or portions thereof, will require a signed warrant and/or subpoena for processing: *customer records containing banking information, including routing numbers, social security numbers, and credit card numbers. (This list may not be all inclusive.)*

Requestor must review and sign prior to document/information being provided:
This request for customer information from ***[Utility]****is being made pursuant to the Washington Public Records Act. Upon signing this statement, the requestor acknowledges that the above information is being requested because they suspect that a particular person to whom the records pertain has committed a crime. The requestor further states that there is reasonable belief that the records being requested could determine or help determine whether their suspicion might be true.*
_____ (signature of requestor)

For Internal Use:
__ Request approved
__ Date information provided
__ Other pertinent information _____.

Signature of Public Records Officer: _____
(A copy of this request and all records provided must be retained in the District's Public Information Request files)

Addendum 8: Summary of Disclosure of Customer Data – Public and Law Enforcement Records Requests (Internal Reference Document)

Disclosure of Customer Data - Public Records Requests and Law Enforcement Records Requests

Information Requested	Is Information Released Based on Method Used to Request (yes/no)?			If "No," Governing law/policy
	General Public Records	Law Enforcement (requires written request[5])	Law Enforcement Warrant or Court Order (all FACTA Data)	
Name	No[1]	Yes	Yes	RCW 42.56.330 - Public Utilities and Transportation
Address	Yes/No[2]	Yes	Yes	RCW 42.56.330 - Public Utilities and Transportation
Mailing Address	No[3]	Yes	Yes	
Telephone Number	No	Yes	Yes	RCW 42.56.330 - Public Utilities and Transportation
Social Security Number	No	No	Yes	42 USC 405
Usage Information - billing period	Yes	Yes	Yes	
Usage Information < billing period	No	No[6]	Yes	RCW 42.56.330 - Public Utilities and Transportation
Email Addresses	No	Yes	Yes	RCW 42.56.330 - Public Utilities and Transportation
Bank Account/Credit Card Numbers	No	No	Yes	FACTA-Patriot Act
Payment information (am't, when pd)	No	Yes	Yes	RCW 42.56.230 - Personal Information Exemptions
Account payment history	No	Yes	Yes	RCW 42.56.230 - Personal Information Exemptions
Type of payment (credit card, cash)	No	Yes	Yes	RCW 42.56.230 - Personal Information Exemptions
Billing statements	No	Yes	Yes	RCW 42.56.230 - Personal Information Exemptions
Customer account notes	Yes/No[4]	Yes	Yes	RCW 42.56.230 - Personal Information Exemptions
Driver's License	No	Yes	Yes	RCW 42.56.230 - Personal Information Exemptions

[1] When requesting the name of a person at an address, the address is exemptible, therefore the name becomes exemptible

[2] No, unless the address is provided in conjunction with a request for usage information

[3] RCW 42.56.330 exempts "addresses", and each utility should discuss with their legal counsel if they want to apply this exemption when dealing with "mailing addresses."

[4] Depends on the content of the note, and if it contains exemptible information

[5] Written request and purpose must be in accordance with Law Enforcement statute RCW 42.56.335

[6] Individual utility decision to release information to law enforcement that is less than the billed usage

This is intended to be guide only. Please consult with your legal council for interpretation of governing laws

Addendum 9: Sample Billing History Report with RCW 19.29A.110 Disclaimer (Customer/Recipient Facing)

12 Month Billing History Report

Premise Address: 123 Main Street
Meter No. 12345

Start Date	End Date	Start Read	End Read	KWH	# of Days	Total Amount
06/24/2016	07/25/2016	65572	66307	735	31	$72.03
05/25/2016	06/24/2016	64964	65572	608	30	$62.05
04/25/2016	05/25/2016	64467	64964	497	30	$53.81
03/25/2016	04/25/2016	63829	64467	638	30	$64.84
02/25/2016	03/25/2016	62793	63829	1036	31	$93.24
01/25/2016	02/25/2016	61474	62793	1319	29	$115.38
12/24/2015	01/25/2016	58870	61474	2704	31	$218.73
11/24/2015	12/24/2015	56711	58770	2059	32	$169.74
10/25/2015	11/24/2015	55507	56711	1204	30	$106.28
09/24/2015	10/25/2015	54976	55507	531	30	$56.90
08/25/2015	09/24/2015	54337	54976	639	30	$63.26
07/25/2015	08/25/2015	53511	54437	826	31	$73.29

IMPORTANT MESSAGE TO ALL RECIPIENTS OF THIS REPORT

The information contained in this report is subject to RCW 19.29A.110, which prohibits its use for commercial or marketing purposes. By receiving this information, you are acknowledging it will be used only as expressly permitted by this RCW.