VALLEY CLEAN ENERGY ALLIANCE

Consent Agenda – Item 8

TO: Valley Clean Energy Alliance Board of Directors

FROM: Mitch Sears, Interim General Manager
Gary Lawson, Sacramento Municipal Utility District (SMUD)

SUBJECT: Data Privacy Policy Revision

DATE: April 25, 2018

RECOMMENDATION

Staff recommends the Board adopt a resolution that approves the attached revision to the VCEA Data Policy.

BACKGROUND

On January 18, 2018 the Board approved the VCEA Customer and Data Policies. Staff has determined that a sentence in the original Data Policy implies that customer data can be removed from the CCA's data management system. The nature of the CCA data transaction with PG&E is such that data for all customers within the CCA service territory is updated on a weekly basis with customer data supplied from PG&E, as part of the CPUC-approved process. VCEA is not able to exclude individual customers from this process. The customer data is protected per the originally approved data policy. However to avoid confusion regarding customer data storage, VCEA recommends the revised policy language shown in redline in Attachment A.

Following Board approval, the redline changes will be accepted and the updated policy will be posted to VCEA's website.

REQUESTED ACTION

Adopt a resolution that approves the revised Data Policy as shown in Attachment A.

ATTACHMENT A

DRAFT

Valley Clean Energy Alliance

Data Policy

~~1/5~~4/16/2018

Table of Contents

1 Privacy Policy

Notice of accessing, collecting, storing, using and disclosing energy usage information

Valley Clean Energy Alliance (VCEA) is committed to protecting your privacy, and as such we comply with the California Public Utilities Commission's (CPUC) "Rules Regarding Privacy and Security Protections for Energy Usage Data" (found here: http://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M026/K531/26531585.PDF).

Data we collect and how we use it

We collect from Pacific Gas & Electric (PG&E) the following information regarding electricity customers within our jurisdictional territory: name, address, phone number, email address, account information, and electric usage information (collected from the customer's meter). This personal information is used only for core VCEA business, for example planning for and providing electricity, customer service, generating charges for your bill, and VCEA service improvement. Your personal data is only kept for as long as is necessary for business purposes.

As you use the VCEA web site, we collect information automatically sent to us by your browser, as well as information about your usage of the site. The links that are clicked on, the pages that are viewed, and time spent on the site are some of the usage statistics and information used in composing web site analytics and reports that help us measure the usefulness of our site. One of the pieces of data automatically sent to us is your IP address. Your IP address is an internet protocol address number automatically assigned to you when you're using the internet. It is logged by our servers and is used to provide web-related services for you, and analytics to VCEA. We do not associate your IP address with personal customer data that we receive from PG&E.

General security protections

As required by the CPUC, VCEA uses appropriate administrative, technical and physical safeguards to protect your information from unauthorized access, including: reasonable employee training, independent audits and annual reporting activities.

De-identified information

De-identified or aggregated information is not subject to privacy restrictions, and VCEA may use or share such information when the data is sufficiently de-identified or aggregated to the point where it is no longer personally identifiable.

Individual choice and access

VCEA will provide to you, upon request, access to your personal information collected by VCEA, which we can update or correct with your input.

VCEA only collects the minimum information needed to provide services to our customers. ~~If you do not wish us to collect and store your information, we may not be able to deliver the associated service(s).~~

Children's privacy

We do not monitor or track the ages of the visitors to our website, but we realize that children under the age of 18 may be interested in the information offered on our website. We ask that parents monitor their children's use of our website and prohibit them from submitting personal information to our website.

California Do not track disclosures

Your browser may have a "Do not track" setting, but unfortunately there is not yet a common understanding of how to interpret this signal, so VCEA's website does not currently respond to browser "Do not track" signals.

Cookies

The VCEA website uses cookies to enhance our customers' web browsing experience. Cookies are small text files placed temporarily on your computer by a web server. VCEA does not collect personal data from cookies, as they are only used to directly provide a customer-friendly web experience.

Google Analytics and web service providers

VCEA website may utilize web-based third party service providers to collect and analyze web usage and traffic. These third parties are listed below with a description of why and how VCEA uses their services. They have their own privacy policies and may collect personal information in accordance with their own data collection policies and practices.

VCEA uses Google Analytics to improve our web-based service offerings, and in order to do that Google Analytics collects your device's IP address (rather than your name or other identifying information), and we do not combine the information collected through Google Analytics with any other information you or PG&E may have provided to us. Google cookies may be used to collect web site usage information such as how often users visit this site, what pages they visit, and what other sites they visited prior to coming to this site. Learn more about how we and Google use this information at http://www.google.com/policies/privacy/partners/.

Hotjar provides VCEA with a different kind of analytics than Google, but collects similar information. Hotjar cookies may be used, but VCEA does not combine the information collected through Hotjar with any other information you or PG&E may have provided to us. Learn more about Hotjar and their privacy practices at https://www.hotjar.com/privacy.

Third parties

In order to provide the services to which you have subscribed, VCEA may utilize third party service providers. VCEA holds these third parties to the same high privacy standards we have

set for ourselves. We only share with these entities the minimum amount of information necessary to provide the services we require of them, and they are not permitted to use the shared information for any other purpose.

In rare circumstances, VCEA may be forced to share your identifiable information with other third parties in accordance with CPUC rules and orders, as well as state and federal law. We may also need to do this during situations involving an imminent threat to life or property. Other than for these rare circumstances, VCEA will not release personal information about you to any other person or business for any secondary purposes without your written consent.

Effective date and updates

The effective date of this policy is [ENTER DATE]. A reminder notice of this policy will be provided on an annual basis to customers via an on-bill message guiding customers to the most updated version on our website at [LINK HERE]. We will communicate any changes through a prominently posted notice on our website and through the aforementioned annual notice to customers. Previous versions of this policy can be found at [LINK HERE].

Accountability

Customers having any questions or concerns regarding the collection, storage, use, or distribution of customer information, or who wish to view, inquire about, or dispute any customer information held by us or limit the collection, use, or disclosure of such information, may contact [ENTER PERSON AND CONTACT INFO HERE].

Type of Data Collected		General Data Practices		Data Sharing	
	**contact:** name, mailing address, email, or phone number		**data retention:** explicitly stated duration of retention for personal data collected		**affiliates:** affiliates and subsidiaries bound by the same privacy practices
	**computer:** IP address, browser type, or operating system		**user control:** users allowed to access and correct personal information		**contractors:** third party contractors bound by the same privacy practices
	**interactive:** browsing behavior or search history				

2 Security Breach Policy

Purpose

This Security Breach Policy ("Policy") has been developed to provide for a consistent response to security breach incidents involving VCEA sensitive and confidential data. The goal of this Policy is to ensure that VCEA responds appropriately to security breaches and ensures that the appropriate communications are taking place when necessary.

Scope

This document is applicable to all directors, officers, and employees of VCEA and any other individual or entity acting for or on behalf of VCEA, whether operating inside or outside of the United States (collectively "Covered Persons"). Third parties, including but not limited to contractors, consultants, agents, intermediaries, and joint-venture partners, must be informed about this policy and agree to comply with its tenets.

Definitions

Covered Information: any usage information obtained through the use of the capabilities of Advanced Metering Infrastructure when associated with any information than can reasonably be used to identify an individual, family, household, residence, or non-residential customer, except that covered information does not include usage information from which identifying information has been removed such that an individual, family, household or residence, or non-residential customer cannot reasonably be identified.

Data quality & security

VCEA is committed to protecting the confidentiality, integrity, and availability of Covered Information. VCEA ensures, to the extent practicable, that collected information is accurate, relevant, timely, and complete in order to maintain as high a level of data quality as possible.

VCEA implements reasonable administrative, technical, and physical safeguards to protect Covered Information from unauthorized access, destruction, use, modification, or disclosure.

Security systems and monitoring

VCEA uses reasonable administrative, technical and physical safeguards and procedures, as well as state of the art security systems as detailed in the system security plan, to monitor its information systems for anomalies and security events that may indicate an incident or breach.

VCEA requires third party service providers to deploy industry standard security controls and perform adequate security status monitoring of the environment and systems used to support VCEA.

Incident handling

When a security incident is believed to have been discovered, support staff will contact their supervisors and the contract manager (if applicable) in order to make management aware as soon as possible. Management will appoint an incident commander, who will be responsible for officially declaring an incident and directing the response (Incident Commander).

Upon determination that an unauthorized person obtained access to or compromised VCEA data or systems, the Incident Commander may direct staff to take the following actions, considering the nature of the event and the presence of any exigent circumstances:

- Assess the scope and character of the incident
- Document the details of the incident and VCEA's handling of the incident
- Begin an incident handling log
- Direct the acquisition, securing, and preservation of evidence
- Contain the incident
- Eradicate the cause of the incident
- Restore the integrity of the system/recover affected systems
- Mitigate the ability for the incident to reoccur/remediate any associated security vulnerabilities

Notification of breach

Once VCEA has identified the type and scope of the information compromised or accessed by an unauthorized person, VCEA will notify the appropriate parties as described in the following sections.

VCEA Customers

Due to the nature of VCEA's work with its Customers, it is possible that PII related to a customer may be breached. If this occurs, VCEA will assess the need to contact the affected Customer or Customers. However, as VCEA does not collect the data elements that require mandatory breach notification in the state of California, it is not anticipated that notification will be required by law. Final determinations regarding mandatory breach notifications will be made by VCEA Legal Counsel.

Law enforcement

If VCEA feels that the information is likely to be misused, or if it is believed to otherwise be a benefit by doing so, VCEA will contact local law enforcement, report the incident, and ask for a copy of the report. VCEA may also contact the local office of the Federal Bureau of Investigations (FBI).

If a law enforcement investigation is opened, VCEA will consult with the applicable agency or agencies regarding the timing and content of any required notifications to avoid compromising or impeding the investigation.

If law enforcement informs VCEA that notification would jeopardize its ability to conduct an investigation and requests that VCEA delay notification, such notice from law enforcement will be in writing and VCEA will delay notification for the period requested by law enforcement. If VCEA determines that the delay is patently unreasonable, VCEA will notify law enforcement that the applicable state agencies and individuals will be notified within a reasonable time frame.

CPUC

In the event of a breach affecting the Covered Information of more than 1,000 customers, VCEA will send a notification of the breach to the Executive Director of the CPUC within two weeks of the detection of a breach or within one week of notification by a third party of such a breach. VCEA will also send notification of a breach to the Executive Director of the CPUC if specifically requested by the CPUC.

Evaluation and response

Once the incident has been confirmed to be resolved, the Incident Commander will also ensure the following actions take place:

- Report the findings and actions taken in response
- Conduct a lessons learned session to determine if response was appropriate and if additional changes are needed
- Recommend policy updates if necessary

Notification language

The text of all notifications will be approved by VCEA management.

Notifications will contain all information and data elements that are required by law and will be distributed as prescribed by the same.

Accountability and auditing

VCEA will file an annual report with the CPUC's Executive Director within 120 days of the end of the calendar year to notify the CPUC of all required notifications. The report will detail the number of demands for disclosure of customer data pursuant to legal process or situations of imminent threat to life or property. The report will also contain a description of all security breaches in the calendar year that affected Covered Information, the number of authorized third parties accessing Covered Information, as well as any known violations of or instances of non-compliance to CPUC rules or contractual provisions experienced in the calendar year, with a detailed description of each instance.

VCEA will make available to the CPUC upon request or audit:

- Privacy notices provided to customers
- Internal privacy and data security policies

- The categories of agents, contractors, and other third parties to which VCEA discloses customer information for a primary purpose (VCEA does not disclose customer information for secondary purposes)

VCEA will provide training on an annual basis to all employees with access to Covered Information. Training will cover topics such as privacy, information security and data quality.

VCEA will conduct an independent audit of its data privacy and security practices every three years or whenever required by the CPUC. The audit will monitor compliance with data privacy and security commitments, and VCEA will report the findings to the CPUC.