KENTUCKY POWER
A unit of American Electric Power

Kentucky Power
101A Enterprise Drive
P O Box 5190
Frankfort, KY 40602-5190
KentuckyPower.com

HAND DELIVERED

June 13, 2016

Aaron D. Greenwell
Acting Executive Director
Public Service Commission
211 Sower Boulevard
P.O. Box 615
Frankfort, KY 40602-0615

RE: Consideration of the Implementation of Smart Grid and Smart Meter Technologies; Case No. 2012-00428 (To be filed in the Company's General Correspondence File)

Dear Mr. Greenwell:

Pursuant to the Order issued in this case on April 13, 2016, Kentucky Power Company (KPCo or Company) submits the following information related to four specific requests from the Kentucky Public Service Commission (Commission):

1. Kentucky Power shall develop policies and procedures that provide customers access to historical information regarding their energy use and tariff rate and shall endeavor to provide this information to customers in as close to real-time as practical. Furthermore, KPCo shall provide aggregated information to the Community Action Council for Lexington-Fayette, Bourbon, Harrison, and Nicholas Counties, Inc. (CAC) upon its reasonable request.

Response: The Company's website (www.kentuckypower.com) offers customers online access to their account information. Customers can view bills (with current tariff information) and payments, up to 36 months of energy usage and sign up to receive proactive billing, payment and outage notifications. The most recent billing information is generally available on the Company's website on the day following a meter reading.

KPCo participates in the Green Button Initiative which provides residential and commercial customers an easy, consistent method to download usage data. Customers can also export data into a spreadsheet format for their personal use and analysis. Data fields available include billing cycle dates, kWh usage, and bill amount for residential and smaller commercial accounts. In addition to these fields, larger commercial account data includes metered and billed kW and kWh, load factor, and cents/kWh.

Kentucky Power
101A Enterprise Drive
P O Box 5190
Frankfort, KY 40602-5190
KentuckyPower.com

Kentucky Power also offers proactive billing and payment alerts. Customers enrolling for such alerts are notified when their bill payment is coming due, past due, or a payment has been made. Similarly, customers can receive outage alerts when the Company believes the customer's power is out.

Company tariffs are available online at https://www.kentuckypower.com/account/bills/rates/KentuckyPowerRatesTariffsKY.aspx.

The Company will provide aggregated information to CAC "after it provides a reasonable basis for requesting the information."

2. Kentucky Power shall develop internal policies and procedures governing customer privacy and customer education.

Response: Kentucky Power does not currently have smart meters and does not collect customer consumption data or other customer information through a Smart Grid. Customer consumption data or other customer information that KPCo obtains by other means is protected in accordance with existing policies.

See Exhibit A for Kentucky Power's internal policy on the handling of electric service accounts. This policy outlines the basic handling of all customer information. See also the following link for the customer privacy policy online at https://www.kentuckypower.com/privacy.aspx. Exhibit B provides the Company's PII (Personally Identifiable Information) Data Privacy Protection Policy. These policies exemplify the Company's long experience in collecting customer information and protecting it and our customers' privacy.

Kentucky Power's internal customer education policy with regard to Smart Grid and smart meters, including appropriate education activities for deployment of smart meters and other Smart Grid components, including Distribution Automation – Circuit Reconfiguration (DACR), Volt VAR Optimization (VVO) and Supervisory Control and Data Acquisition (SCADA), is attached as Exhibit C.

3. Kentucky Power shall certify to the Commission that it has developed internal cybersecurity procedures.

Response: Kentucky Power certifies to the Commission that it has developed written cybersecurity policies and procedures. These cybersecurity policies and procedures are approved by management and address known and reasonably foreseeable cybersecurity risks. The policies and procedures incorporate essential elements of Kentucky Power's

KENTUCKY POWER
A unit of American Electric Power

Kentucky Power
101A Enterprise Drive
P O Box 5190
Frankfort, KY 40602-5190
KentuckyPower.com

system that may be susceptible to cyber threats, in conjunction with plans for hazard mitigation, emergency response and recovery and other relevant arrangements for continuity of service.

In addition, Kentucky Power agrees to meet with the Commission every two years, through the Track Meeting process, to make a presentation describing its cybersecurity procedures.

4. Kentucky Power shall develop internal policies and procedures regarding Smart Grid investments.

Response: See Exhibit D for KPCo's internal policy and procedure with regard to Smart Grid investments.

If there are any questions regarding this information, please do not hesitate to call.

Sincerely,

Ranie K. Wohnhas /by SAG

Ranie K. Wohnhas
Director, Regulatory and Finance

EMPLOYEE POLICY FOR PROPER HANDLING OF ELECTRIC SERVICE ACCOUNTS

All information contained in the Customer Information System (MACSS) is confidential and proprietary. The information contained therein should only be discussed with other Company employees, approved contractors, credit agencies and regulatory agencies when necessary to perform your job duties. Sharing confidential customer information with any other parties shall require written consent of the customer.

Customer Records are property of AEP and are not to be used to obtain information for personal gain. It is prohibited to transfer customer information from your workstation computer to any other computer outside AEP.

Employees having direct access to electric service accounts through the Customer Information System (MACSS) or Contact Center Desktop (Virtual Agent) are **prohibited** from performing transactions or activities that impact the integrity and accuracy of the account information and billing. This prohibition without limitations includes the following:

a. Your own AEP account(s) or your own premise of record;
b. Accounts of your immediate household members;
c. A relative's account;
d. The electric service account of an individual with whom you have a personal relationship or association (other than an immediate family member or a close relative) where the nature of the relationship creates a potential conflict of interest.
e. The electric service account of an employee who works within your same section or work group regardless of work location, or an employee who works at the same Customer Operations Center. It is permissible for you to perform record maintenance within standard company guidelines on all other employee electric service accounts.
f. Employees are prohibited from accessing customer accounts without specific cause such as account maintenance, transaction completion or obtaining information for the customer of record.

Employees may conduct business on their own account through the Internet (AEPOhio.com, SWEPCO.com, KentuckyPower.com, etc.) or the automated telephone service (IVR) as those applications are controlled for all customers.

If you are ever in doubt concerning whether a particular transaction is permitted under this policy, you should contact your supervisor for clarification. If approval is given, a permanent note must be made on the account documenting the conversation by the supervisor granting approval.

Any violations of these guidelines can result in disciplinary actions, up to and including discharge for the first offense.

Protect Customer Account Information

All information contained in the Customer Information System (MACSS) database is confidential and proprietary. The information contained therein should only be discussed with other Company employees or persons who are not employees when necessary to perform your job duties as set forth below.

The Company recognizes that on occasion, someone other than the customer of record may contact you to seek information, open, close or make other adjustments/transactions to an electric service account. For example, a customer of record often authorizes a spouse, close relative, attorney, roommate or landlord to conduct this type of business. In other cases, the caller may be a representative from a governmental agency or community group with whom the Company has an established, working relationship seeking payment or disconnect information on a customer account other than their own. You are permitted to provide requested information, open, close or make other adjustments to an electric service account when the following actions are taken:

If the caller requests account information or a transaction to be performed on the account, the caller must provide the account number or social security number of the account holder, in addition to their relationship to the account holder before account information is released or the transaction performed. On established accounts, which are accessed by the meter number, address or telephone number, it is acceptable to verify only the last four digits of the social security number. This rule does not apply to outage tickets or streetlight outages.

In rare circumstances where the caller cannot provide either the account number or the social security number, however they can provide other types of information on the account, approval must be obtained from the Supervisor or Lead before actions are taken on the account or information provided. A Supervisor or Lead must note the account as to why information was provided.

In some cases, written authorization from the customer may be required before information can be given to the caller.

If the caller is requesting information be mailed to a third party, the Customer Information Release Form must be completed and submitted to the Company. Once the signed form is received, the Customer Operations Billing (COB) group will send the requested information.

Customer Records are property of AEP and are not to be taken home or used to obtain information for personal gain. It is also prohibited to transfer customer information from your workstation computer to any other computer outside AEP.

Good judgment should always be used prior to providing others with information on an account. If you are ever in doubt as to the appropriateness of releasing customer account information to someone other than the customer of record, contact a supervisor for clarification.

PII Data Privacy Protection Policy

Title:	PII Data Privacy Protection Policy	**Date:**	**March 14, 2016**
Owner:	Julie Rutter, Chief Compliance Officer	**Sponsoring Area(s):**	Ethics & Compliance; Security; Legal; IT; Human Resources; Procurement; Customer Services, Marketing & Distribution Svcs.; Accounting

Policy Statement:

AEP recognizes the importance of having effective and meaningful privacy protections in place when it collects, uses, retains, discloses, and/or destroys Personally Identifiable Information ("PII"). These protections are necessary to instill confidence in AEP's employees, contractors, agents, and customers, who may furnish PII to AEP and/or are themselves subject to local privacy and data protection laws, as well as to ensure AEP's own compliance with such laws.

AEP shall apply protective measures when handling PII under its control or in its possession. The purpose of this PII Data Privacy Protection Policy ("Policy") is to establish privacy standards applicable to PII throughout AEP.

Where applicable, AEP will comply with more restrictive local or state privacy and data protection laws or regulations, in addition to the Policy.

Detail:

Scope

This Policy applies to the collection, use, retention, disclosure, and destruction of PII by AEP and any third-party contracted agents to whom AEP supplies PII as a consequence of the contractual relationship. AEP, or any of its business units, departments, or work groups, may develop and/or use more detailed guidance or procedures to address privacy concerns involving individual AEP programs, activities, or initiatives, so long as they comply with this Policy. If AEP personnel are unsure whether information qualifies as PII under the Policy, or whether particular guidance or procedures are in compliance with this Policy, they should consult AEP Ethics & Compliance.

This Policy supersedes any previous policy of AEP concerning Privacy and Data Protection and/or PII Governance. In the event of any conflict or inconsistency between this Policy and any other materials previously distributed by AEP, this Policy governs.

Definitions

While various jurisdictions may employ differing definitions with which AEP may be required to comply, AEP nevertheless recognizes that its employees need guidance on the types of information to classify and protect as PII. For purposes of the Policy, the following terms and definitions apply:

1. Personally Identifiable Information ("PII")

AEP currently treats as PII an individual's first name or initial with last name, plus any one of the following additional data elements, when either the name or the data elements are not encrypted:

- Social Security Number
- Driver's License number
- State or federal government-issued ID number
- Passport number
- Biometric data (including but not limited to fingerprint, DNA, voiceprint, or retinal scan)
- Personal credit card number
- Bank account or debit card number, along with any required security information or password required for access

2. Data Owner

A Data Owner includes the AEP business unit, department, or work group that collects, uses, or retains any PII data, in either hard copy or electronic format, for use in any legitimate business purpose. The term Data Owner also includes the vice president in charge of that business unit, department, or work group.

Unless otherwise stated below, and while others may be responsible and/or consulted or relied upon for certain tasks relating to the Policy, the Data Owner is accountable for ensuring that this Policy is followed with regard to all PII collected, used, retained, or disclosed by that Data Owner.

Policy

1. PII Inventory

Each Data Owner shall ensure that a complete inventory of its PII shall be completed on or before November 25, 2015. At least once annually (not later than December 31st of each subsequent year), the Data Owner shall review the inventory and confirm that it continues to be accurate and complete, or update the inventory if it is no longer accurate or complete. The inventory shall note, at a minimum:

- The types and description of PII data in the Data Owner's possession; and
- All locations, both physical and electronic, where the Data Owner's PII is stored; and
- A description of how the PII is presently secured; and
- The roles of the individuals having access to, and accountability for, the PII data; and;
- The business purpose for using the PII data; and
- Locations to which the data may be sent, both internally and externally, and the business purpose for such transfers.

The Office of Ethics & Compliance shall be responsible for owning and maintaining the inventory and confirming that Data Owners provide the required annual confirmation and/or updated information described above.

2. Legitimate and Fair Use

AEP shall only collect, use, retain, disclose, or destroy PII by lawful and fair means, in accordance with applicable laws, regulations, and other legal requirements, and fully observing the legal rights of individuals. AEP shall only obtain or use PII to fulfill AEP's legitimate business purposes. AEP shall obtain and use the minimum amount of PII necessary and, whenever possible, shall rely instead upon anonymized or aggregated information to accomplish its business objectives. AEP expressly prohibits any unauthorized collection, use, or disclosure of PII by AEP employees, contractors, or agents.

3. Notice to Individuals

AEP shall strive to ensure that its collection, use, retention, disclosure, and destruction of PII is transparent. AEP shall take reasonable steps to furnish individuals with an appropriate form of notice informing them of the following, unless to furnish such notice would be impracticable or impossible under the circumstances:

(i) the purposes for which AEP collects and uses the PII;
(ii) how to contact AEP if the individual has any issues or concerns about AEP's use of PII; and
(iii) the means and methods by which AEP protects the PII.

Notices shall be provided in plain language, in written form, and before PII is first collected or, if that is not possible, as soon as practicable thereafter. Data Owners in charge of individual AEP programs, activities, or initiatives that will result in the collection, use, retention, and/or disclosure of PII shall decide the appropriate mechanism for imparting notice, taking into account the relationship with the relevant individual, the circumstances under which the PII is collected, and other relevant factors. For the avoidance of doubt:

Where AEP obtains PII from individuals by means of AEP job application or requests for service, AEP shall include within the pertinent documentation appropriate written notices.

Where AEP captures PII by means of benchmarking surveys, questionnaires, and related research tools, AEP shall include within the surveys and tools appropriate written notices and only proceed to collect and use the PII captured via such devices where the respondent has agreed to such processing. In the absence of such agreement, AEP should not process the PII contained in the relevant survey or tool.

Where AEP obtains PII from individuals online, AEP shall furnish such individuals with an appropriate form of notice that takes into account the manner by which the PII is collected, which may take the form of an online privacy statement, policy, or other informational disclosures.

4. Information Integrity

AEP shall only use PII in accordance with any notices furnished to or consents obtained from individuals, and shall not later process PII for any additional, incompatible purposes unless required or expressly permitted by law or after furnishing additional notice to the individual. AEP shall only collect PII that is relevant in light of the business purposes the PII is meant to serve and shall employ reasonable means to keep the PII accurate, complete, up-to-date, and reliable. AEP materials and forms used to collect PII shall be prepared in such a manner that only pertinent PII is captured.

5. Information Security

Data Owners shall implement appropriate administrative, technical, and organizational measures, including those appearing in AEP's current security policies and standards, to safeguard their PII against loss, theft, misuse, unauthorized access, modification, disclosure, or destruction. Data Owners shall only retain PII for so long as legally and reasonably required to serve AEP's legitimate business needs. PII subsequently shall be anonymized, deleted, or destroyed, subject to AEP document retention guidelines, legal holds, and any applicable legal or regulatory records retention requirements.

Data Owners shall restrict access to PII to only those AEP personnel or third-party contracted agents who have a legitimate business need for such access given their roles and responsibilities. At least once annually, Data Owners shall perform reviews of all electronic and physical access to the Data Owner's PII, and shall terminate the access of all employees, contractors, and other individuals who no longer require such access to complete their assigned job responsibilities. Data Owners shall confirm to the Office of Ethics & Compliance the completion of such access review, and the termination of unneeded access, not later than December 31st of each calendar year.

Data Owners shall only disclose PII to third-party contracted agents who expressly agree to and are capable of protecting the PII to at least the same degree as AEP. In the event a Data Owner learns or reasonably believes that a third-party contracted agent is failing to apply adequate privacy protections to PII, the Data Owner shall take immediate steps to require compliance, or shall terminate the relationship with the third-party contracted agent. In all new or existing contractual agreements, the Data Owner must ensure that the third-party contracted agent is providing PII protections as described herein, and must further ensure that AEP Cyber Security has completed or will complete a third-party risk assessment of the third-party contracted agent.

PII maintained in hard copy form shall be protected, at a minimum, by remaining in the physical possession of the Data Owner or a designee, or locked within a secure container at all times. If the PII is in transit, it shall remain in the physical possession or control of the Data Owner or a designee, or locked within a secure container and out of sight at all times.

PII maintained in electronic form shall be protected, wherever possible, by encryption. Data Owners shall work with AEP Cyber Security and/or Audit Services to confirm that protection measures in place to protect their electronic PII are sufficient to protect the data, whether encrypted or otherwise.

All electronic transfers of PII within AEP shall be protected, wherever possible, by encryption.

All electronic transfers of PII external to AEP shall be protected, at a minimum, by encryption.

Upon termination of any relationship with a third-party contracted agent who at any time received PII from AEP, the Data Owner shall obtain written confirmation from the third-party contracted agent of the complete return, disposal, or destruction of all PII data previously supplied.

6. PII Incident Response

AEP shall maintain a PII Incident Response Plan (the "Plan") which will establish an Incident Response Team (the "Team") and set forth the Team's roles and responsibilities in the event that PII is involved in any security event, incident, or breach as those terms are defined in the Plan. The Plan shall be co-owned by the Chief Compliance Officer and the Chief Security Officer. The Plan owners will ensure that the Plan is reviewed at least once annually and revised as needed. The Plan owners will further ensure that the members of the Team conduct a drill or training exercise on the Plan at a minimum at least once annually.

7. Information Access and Correction

AEP shall allow individuals to review and confirm the validity of the PII that AEP holds relating to that individual, unless such access would be inappropriate or unnecessary. Instances where access may legitimately be denied include where such access would materially prejudice AEP's legitimate business interests or legal rights, adversely affect the privacy rights of third parties, or impose a disproportionate burden upon AEP given the attendant privacy risks to the individual. Where access is refused, AEP will inform individuals of the reasons for the denial. In the event that an individual establishes to AEP's satisfaction that his/her PII is inaccurate or incorrect, AEP shall promptly correct or amend the relevant PII.

8. Disclosures to Non-Agent Third Parties

AEP places substantial importance on protecting the confidentiality of PII. For that reason, AEP shall inform individuals whenever their PII may be disclosed to non-agent third parties, if practicable. AEP will not disclose PII to non-agent third parties except as required by law or other governmental order, or as specifically authorized by the individual owner of the PII.

9. International Transfers of PII

Prior to the international transfer of PII, AEP shall implement any additional measures that are required under any applicable laws regulating such transfer and only transfer PII in furtherance of AEP's own legitimate business needs. If AEP personnel need additional guidance regarding international transfers of PII, they should consult AEP Ethics & Compliance.

10. Compliance

AEP shall maintain an active program to ensure compliance with and awareness of the Policy. Data Owners shall ensure that all employees and contractors who have access to PII data receive training and/or instruction at least annually regarding this Policy and any associated or supporting policies, procedures, or guidelines established by the Data Owner to protect PII.

All AEP employees, contractors, and third-party contracted agents are required to adhere to this Policy and any associated or supporting policies. Failure to do so may be grounds for disciplinary action, up to and including termination.

11. Enforcement and Complaint Resolution

AEP is committed to assisting individuals in protecting their privacy and in providing opportunities to raise concerns about the processing of their PII. Complaints relating to this Policy should be raised pursuant to the procedures set forth in AEP's Principles of Business Conduct.

Review / Revision:

Approved By:

Julie A. Rutter	Senior Counsel & Chief Compliance Officer	March 14, 2016
David M. Feinberg	EVP, General Counsel & Secretary	March 14, 2016
Lana L. Hillebrand	SVP & Chief Administrative Officer	March 14, 2016
Andrew B. Reis	VP, Audit Services	March 14, 2016

Kentucky Power – Customer education and information on gridSMART® technologies

Kentucky Power believes that clear communication is essential to customers' ability to achieve maximum benefits of new smart grid technologies. Kentucky Power will thoroughly communicate with customers about its smart grid plans and installations, as well as the benefits customers may receive from these investments.

Kentucky Power will develop and implement specific communication and education plans for its larger programs to facilitate transparency, customer understanding and acceptance.

Overall, Kentucky Power's approach will be:

- To communicate directly to individual customers about activities and programs that directly and specifically affect them.
  Example: If a smart meter is to be installed at a specific premise, Kentucky Power will communicate directly with the resident through personal channels, including but not limited to direct mail, bill inserts, phone calls, door hangers, texts, emails, advertising, website, social media, a dedicated customer support help line, etc.

- To communicate with employees, customers, regulators, community leaders and other stakeholders on a larger scale, including mass media, about technologies and infrastructure investments that benefit customers as a whole.
  Example: If Kentucky Power were to roll out smart grid technology or technologies, such as Volt VAR Optimization (VVO), Distribution Automation – Circuit Reconfiguration (DACR) or Supervisory Control and Data Acquisition (SCADA), the Company may communicate directly with customers on affected circuits, but also it will communicate and educate general audiences using tools and tactics such as news releases, editorials, displays at home shows, website, social media, emails, bill inserts, etc.

Key messages (may vary relative to specific technology being installed):

- Kentucky Power is investing in (name technology) to improve service in your area.
- This new technology will improve service quality and/or reliability and will provide more data about your energy service and/or use.
- Kentucky Power values your privacy and the security of your energy use and account information and works to keep that information private and safe.

AEP Smart Grid Investment Strategy / Evaluation Process

AEP's operating companies seek to invest in existing and new Distribution gridSMART® technologies with a goal of maximizing customer benefit / experience while managing costs as prudently and effectively as possible. These types of investments are reviewed from several different perspectives and shared with external stakeholders, including commission Staff, as part of any regulatory request and/or filing.

Overview of Distribution Technologies

1. Automated Meter Reading (AMR)

Automated Meter Reading (AMR) is a one-way communication technology that allows the electric provider to automatically collect consumption, demand, and status data from electric meter devices and transfer that data to a central database for billing, troubleshooting, and analyzing. This technology primarily allows the electric provider to reduce the expense of periodic trips to each physical location to read a meter; readings are acquired primarily by radio frequency communication via vehicles driving within a reasonable distance of the meter devices.

Another advantage is that billing can be based on near real-time consumption rather than on estimates based on past or predicted consumption. This timely information coupled with analysis can help both electric utility providers and customers better control the use of electricity through improved data. AMR technologies can be based on several platforms – telephone (wired and wireless), radio frequency (RF), or powerline transmission.

Kentucky Power currently has AMR installed across its service territory.

2. Advanced Metering Infrastructure (AMI)

Advanced Metering Infrastructure (AMI) is comprised of digital electric meters and a two-way wireless communication system that provides a facility for meter communication and transporting meter data. AMI also includes a series of back-office systems that securely oversee

AEP Smart Grid Investment Strategy / Evaluation Process

the meters and associated network, collect meter data, and then process and store meter data for use by the utility in a variety of business functions.

AMI meters provide the electric provider with the ability to remotely gather electric meter data at pre-defined time intervals enabling a more robust analysis of aggregated usage information to help Kentucky Power better serve its customers.

The AMI meters can be configured to include service switches to allow the electric provider to disconnect and reconnect electric service, in compliance with Commission rules, without utility personnel having to visit the premises.

AMI meters also expand the parameters of data delivery from beyond usage and demand into other valuable data sources like voltage and temperature. Along with more frequent interval usage data, this provides the electric provider with expanded opportunities to leverage data analytics across numerous areas including improved detection of theft, consumption on inactive meters, detection of failing transformers, incorrectly mapped transformers/customers, and quicker detection and reaction to outages amongst others.

Meters may also be configured with home area network (HAN) interface modules providing a gateway within the premises for customer access to meter data and functions. The HAN is implemented using a wireless technology such as Zigbee to enable the connection of devices to the meter within the premises. Such connection to devices within the home can enable current or future demand-side technologies that allow customers greater flexibility to use energy more efficiently and/or respond to time-of-use rates that may contribute to a generally more efficient power system.

Kentucky Power currently does not have AMI installed anywhere within its service territory.

AEP Smart Grid Investment Strategy / Evaluation Process

3. Volt VAR Optimization (VVO)

The voltage on a distribution circuit can vary from the substation to the end use customer. Although this voltage is within established guidelines, significant energy and demand savings can be achieved by more tightly controlling voltage. Volt VAR Optimization (VVO) provides these benefits by strategically automating the control of capacitors and voltage regulators. With a lower voltage that is more in line with equipment nameplate requirements, customers served from the improved circuits will, in aggregate, realize lower energy consumption year round.

VVO is an energy efficiency program that will reduce energy consumption and demand without any needed interaction or "participation" from the customer. Customer end-use equipment (HVAC, lighting, appliances, etc.) is designed to operate at peak efficiency at a specific voltage. In reality, the equipment typically operates at voltages that are higher than this optimum voltage. Voltage levels are currently maintained using capacitor banks and voltage regulators installed at different points along a circuit. This technology has worked for decades and has proven to be a cost effective way to maintain voltage levels within the required range (120 V +/- 5%). When VVO is added to a conventional circuit, the control system can then more closely control the voltage that is delivered to the meter and, subsequently, to the customer's end-use electrical devices. VVO provides an opportunity to supply voltages that are closer to the design voltage of the end-use equipment and thus increase the efficiency of the customer's load by reducing excess energy. Peak demand and energy usage reductions will average approximately 2 to 4% on circuits where VVO is applied. Customers should realize lower consumption while maintaining the same level of comfort and service. Further, optimizing the voltage supplied will ultimately reduce the amount of capacity and energy required to serve Kentucky Power customers.

VVO utilizes two way communications with substation and line voltage regulating devices and voltage sensors. A control system receives voltage level information from the devices, runs an

AEP Smart Grid Investment Strategy / Evaluation Process

algorithm to determine optimum settings for each device and issues commands for the devices to operate at those levels.

Kentucky Power has installed VVO on 24 circuits, the operation of which is being evaluated and further optimized. In addition, the Company is installing VVO on two additional circuits.

4. Distribution Automation – Circuit Reconfiguration (DACR)

Distribution Automation – Circuit Reconfiguration (DACR) utilizes two way communications and a control system to control substation distribution breakers, reclosers, and switches to restore service automatically to as many customers as possible during circuit outages. The control system receives status information from all of the devices and determines which devices should open to isolate a faulted line section and which devices should close to reconfigure the circuit and restore service to the customers in the un-faulted sections. This technology helps reduce the number of customers impacted by outages and thus improves the System Average Interruption Frequency Index (SAIFI) and System Average Interruption Duration Index (SAIDI) indexes.

Kentucky Power has DACR installed on 6 circuits and is installing it on 20 additional circuits.

5. Supervisory Control and Data Acquisition (SCADA)

SCADA is the system that allows utilities to have real-time situational awareness of both the transmission and distribution systems. Kentucky Power has implemented a new distribution SCADA system, commonly referred to as a Distribution Management System (DMS). Through this system, distribution dispatch operators and engineers, can see the state of the distribution grid for devices that have been enabled and can remotely operate the system when necessary. Circuits that have VVO and DACR equipment installed are examples where real-time

AEP Smart Grid Investment Strategy / Evaluation Process

information is available. As new smart devices are deployed in Kentucky, they are modeled in the DMS system for improved operational and engineering benefits. When outages occur and are detected by smart reclosers or switches, the DMS provides information to the Outage Management System (OMS) which facilitates a more rapid identification of where to dispatch line crews for outage restoration. The addition of the DMS will also help promote and enhance the ability to connect Distributed Energy Resources (DER) on the distribution circuits.

Planning Goals

As stated previously, AEP's operating companies seek to invest in existing and new Distribution gridSMART® technologies with a goal of maximizing customer benefit / experience while managing costs as prudently and effectively as possible. These types of investments are reviewed from several different perspectives and shared with external stakeholders, including commission Staff, as part of any regulatory request and/or filing. A high-level overview of the investment evaluation process is included below.

Distribution gridSMART® Technologies / Programs for Investment Consideration:

- Advanced Metering Infrastructure (AMI)
- Volt VAR Optimization (VVO)
- Distribution Automation – Circuit Reconfiguration (DACR)
- AMI-Enabled Consumer Programs (e.g., Time of Use, Direct Load Control, Prepaid Metering)
- Other evolving Distribution technologies as needed or requested
    - Energy storage

AEP Smart Grid Investment Strategy / Evaluation Process

- Virtual Power Plant
- Distributed generation
- Combined heat and power

Investment Review Considerations

- Quantifiable customer cost-benefit analysis – In evaluating gridSMART® technology options, AEP will consistently complete an internal business case that quantifies the customer costs and benefits for internal evaluation. Based on this evaluation, the analysis will be shared with external stakeholders if/when a proposal is made to move forward with the technology. High-level costs and benefits for consideration include, but are not limited to, the following:
  - Costs for Consideration – Asset investment, asset installation and maintenance, network installation and maintenance, IT system implementation and support, project management
  - Benefits for Consideration – Potential labor savings, credit/collections improvements, data analytics use case-driven revenue enhancements or cost reductions, energy usage and peak load reductions (lower overall customer bill)
- Non - quantifiable customer benefits – In evaluating gridSMART® technology options, AEP will consistently complete an internal review of non-quantifiable customer benefits for internal evaluation. Based on this evaluation, these benefits will be shared with external stakeholders if/when a proposal is made to move forward with the technology. High-level benefits include but are not limited to the following:
  - Enablement of future consumer programs

AEP Smart Grid Investment Strategy / Evaluation Process

- Enablement of customer access to energy usage information (e.g., through web portal) and increased customer control of usage
- Non-quantifiable, customer-focused data analytics (e.g., advanced customer segmentation, customer mapping improvement through voltage analysis, proactive asset health monitoring)
- Improved billing accuracy
- Outage frequency reduction
- Outage duration reduction
- Decreased calls to customer operations centers / improved customer speed of answer times