

FirstEnergy's New Jersey Utility Company Customer Privacy Policy Regarding Protection of Smart Meter Information

November 2019

FirstEnergy's New Jersey utility – Jersey Central Power & Light ("the Company") – takes the responsibility to protect the privacy and security of their customer's information very seriously and that commitment continues with the introduction of smart meters. In addition, the Company places importance on the security and protection of all aspects of its electric system and associated sub-systems, including its New Jersey smart meter system. This Customer Privacy Policy has been developed to describe how the Company protects Sensitive Customer Information related to the use of smart meters.

Sensitive Customer Information includes, but is not limited to, the following:

- Name (contact name, company name, etc.)
- Address
- Interval Energy Usage Data
- Social Security Number
- Employer Identification Number
- Driver's License Number
- Date of Birth
- Credit Card Number
- Bank Account Information
- Government Passport Number

The Company collects and retains Sensitive Customer Information that is reasonably necessary to serve its customers, effectively manage business operations and meet regulatory and compliance obligations. The Company does not sell or share any Sensitive Customer Information to third parties. In addition, it will not disclose a customer's information without prior consent, except as required by law, requested by regulatory agencies and governmental authorities, or for legitimate business purposes (such as credit evaluations). The Company protects Sensitive Customer Information under current privacy protection laws, regardless of meter type.

Using internal and external audit processes, the Company's system is regularly evaluated to ensure that employees are able to access Sensitive Customer Information if necessary to perform their job and only on a need-to-know basis. All employees and contractors who have access to Sensitive Customer Information are required to maintain the confidentiality of that information and have received specialized training in the handling of such information.

No personally identifiable customer information – such as names and addresses, account numbers, credit/collection information or social security numbers – is stored in the Company's smart meters or transmitted across the Company's smart meter communication network. The Company's smart meter communication network is a high security environment that uses multiple layers of protection from unwanted access – including the use of passwords, firewalls, continuous security monitoring and other security controls. In addition, usage data transmitted over the network is encrypted.

All systems and hardware are protected using nationally recognized protocols, controls and standards. Where vendors are involved, they are required to adhere to the Company's security standards and advanced metering infrastructure guidelines published by the North American Energy Standards Board (NAES) and the National Institute of Standards and Technology (NIST).

The Company will continue to monitor any privacy-related issues that may arise and will adjust its procedures and protocols as necessary in order to remain in compliance with any new requirements concerning customer privacy.