FirstEnergy Security Requirements for External System & Service Providers
Version: 2020-07-30

A) Definitions

For the purposes of the FirstEnergy Security Requirements for External System & Service Providers, the following statements apply:

1. Service - The service(s) being procured by FirstEnergy. This term does not apply to any system or service offered by the supplier not in scope to provide the service(s) to FirstEnergy.

2. System - Any technology resources including electronic information, software, computing devices, network devices, or communication services used to create, modify, retrieve, transmit, or store information providing collectively the Service.

3. FirstEnergy Information – Information and data that is considered Sensitive (non-public) as defined by FirstEnergy Corporate Policy 808 and that is:

    a. provided by FirstEnergy to the supplier to provide the service(s) being procured by FirstEnergy; or

    b. developed, gathered, aggregated, or created by the supplier that would be considered protected classes of information such as Personally Identifiable Information (PII), HIPAA, etc.

4. Transmission / Transmit - the act of moving or copying data between two electronic Systems over a network where the underlying network connection is not controlled by the supplier (e.g. the Internet)

5. Transport - the act of moving data between two physical Systems using intermediate, non-network media (e.g., a hard drive, a USB-attached drive, etc.) outside of a security perimeter controlled by the supplier.

B) Cryptographic Requirements

1. All FirstEnergy Information held by the supplier or the supplier's subcontractors is protected while in Transmission or Transport using the Advanced Encryption Standard (AES) with a key length of at least 128 bits or other defined industry standard that offers similar or better protections

2. Systems that use Transport Layer Security (TLS) to Transmit FirstEnergy Information must use the TLS protocols as defined in IETF RFC 5246 (TLSv1.2), IETF RFC 8446 (TLSv1.3), successor standards, or other commonly recognized industry standards

3. Systems that use encrypted tunneled network connections (e.g. IPSEC, VPN, etc.) to Transmit FirstEnergy Information between Systems must use strong industry-standard protocols with an effective security strength of 128 bits or higher (or a functional equivalent) and support strong key exchange and hash functions that are not known to be cryptographically compromised.

4. No System may rely on known-compromised cryptographic algorithms or processes for any encryption or integrity purpose. When an in-use algorithm or process become cryptographically compromised, the supplier must retire its use when practical following industry best practices and responses.

C) Account Lifecycle Management

1. Supplier must ensure that all persons (employees, contractors, third-party suppliers, etc.) who access Systems that contain FirstEnergy Information have authorization to that system and are limited to the privileges necessary to perform job functions. Supplier must ensure that supporting sub-contractors or other providers who access the supplier's Systems are authorized, limited, and reviewed the same as the supplier's employees

2. Supplier must ensure that all privileges to the Service and Systems are periodically reviewed and access that is no longer appropriate is removed.

D) Strong Authentication

1. All accounts for Systems that contain or process FirstEnergy Information must use strong passwords that are changed on a reasonable, periodic basis to maintain the integrity of the access based on industry best-practices such as periodic password changes and complexity for short password (e.g. NIST 800-63B) or long passphrases with long lifetimes (e.g. NIST 800-63B).

2. User passwords on Systems must be stored in such a manner that they are resistant to offline attacks using an industry-standard one-way key derivation function with a standardized hashing function and per-item salting (e.g. salted SHA2, PBKDF2, etc.).

3. Administrative or otherwise elevated access to Systems that contain or process FirstEnergy Information must use a multi-factor authentication system.

E) Data Storage and Processing

1. All FirstEnergy Information provided must be stored and processed on Systems located within the United States, including any storage or processing being provided by a third-party or subcontracted supplier.

2. All FirstEnergy Information must be removed from the supplier's Systems at the termination of business between FirstEnergy and the supplier. This includes any subcontractors or other partners of the supplier.

3. All Systems that store and process FirstEnergy information must be protected from physical attacks and theft using industry-standard best practices (e.g. NIST 800-53R4 PE-3). Physical Access to such Systems must be limited to required personnel.

4. FirstEnergy Information must only be used for the purposes necessary to provide the contracted Service(s). FirstEnergy Information must not be otherwise used for data mining, research, etc.

F) Security Awareness and Monitoring

1. All Systems that store and process FirstEnergy Information must be continuously monitored for unauthorized access, cyber attacks, and other potentially relevant security events, including physical events.

2. The supplier must maintain a cyber security program to collect, detect, analyze, and respond to monitored events of the Service.

3. In the event of a suspected or actual data breach, the supplier must maintain capability to disable the Service(s) or otherwise secure FirstEnergy Information from theft or misuse.

4. The supplier must maintain a process to monitor for security-relevant software updates to any software package used in the Service(s) being provided to FirstEnergy and must install applicable security-relevant updates in a reasonable timeframe after release and testing.

G) Third Party / Subcontractor Responsibilities

1. Any third party or subcontractor used by the supplier directly for the delivery or operation of the Service and its Systems that store or process FirstEnergy Information are compliant with these requirements.