Leitlinie

Herausg.	Schutzklasse	Gültig ab
Geschäftsführung	öffentlich	01.11.2022

Leitlinie zur Informationssicherheit der TEN Thüringer Energienetze GmbH & Co.KG

Die Geschäftsführung der TEN Thüringer Energienetze GmbH & Co.KG hat beschlossen, ein Informationssicherheitsmanagement (ISMS) zu etablieren.

Die in dieser Leitlinie dargelegte Informationssicherheitspolitik der TEN Thüringer Energienetze GmbH & Co.KG definiert die grundlegenden Ziele, Strategien und den Rahmen zur Gewährleistung der Informationssicherheit im Unternehmen.

Die Einhaltung der Vorgaben aus dieser Leitlinie zur Informationssicherheit ist für alle Mitarbeiter der TEN Thüringer Energienetze GmbH & Co.KG und für Dritte verbindlich, die an den Netzbetriebsprozessen beteiligt sind.

TEN Thüringer Energienetze GmbH & Co. KG
vertreten durch die TEN Thüringer Energienetze Geschäftsführungs-GmbH
vertreten durch die Geschäftsführung

Ulf Unger

Frank Peter Tille

Inhaltsverzeichnis

1 Einleitung

Für die TEN Thüringer Energienetze GmbH & Co. KG (nachfolgend TEN genannt) haben die Werte Verfügbarkeit, Integrität und Vertraulichkeit von Informationen einen außerordentlich hohen Stellenwert. Aufgrund der Bedeutung der Informations- und Kommunikationstechnik (nach-folgend IKT genannt) für einen sicheren Betrieb der Energienetze und der gesetzlich vorgegebenen Erfüllung der regulatorischen Anforderungen der BNetzA ist die Sicherstellung der Informations- und IT-Sicherheit ein strategisches unternehmerisches Ziel.

Die Informations- und IT-Sicherheit sind sich rasant entwickelnde Disziplinen. Beinahe täglich gibt es Veröffentlichungen zu neuen Schwachstellen oder Bedrohungen. Zusammengefasst wird dies gern mit der Devise: „Sicherheit ist kein Produkt, sondern ein Prozess". Entsprechend muss sich auch das Informationssicherheitsmanagement der TEN fortlaufend an neue Gegebenheiten und Herausforderungen anpassen. Erreicht wird dies durch einen kontinuierlichen Verbesserungsprozess.
Die Geschäftsführung der TEN ist verpflichtet, auf der Grundlage der einschlägigen gesetzlichen Regelungen ein ISMS aufzubauen, zu betreiben und zertifizieren zu lassen.

2 Rahmenbedingungen

2.1 Kontext

Die vorliegende Leitlinie zur Informationssicherheit bildet den Ausgangspunkt für die darauf aufbauende Struktur zu Richtlinien der Informations- und IT-Sicherheit sowie zu entsprechenden Arbeitsanweisungen, Prozessbeschreibungen, technischen Konzepten und betrieblichen Dokumentationen. Insofern werden mit ihr Ansatz, Ziele und Methoden der TEN zur dauerhaften Gewährleistung einer angemessenen Informationssicherheit im Unternehmen beschrieben.

Die Leitlinie zur Informationssicherheit ist zudem Auftrag an die Sicherheitsorganisation der TEN. Durch die Leitlinie soll sichergestellt werden, dass dem jeweiligen Schutzzweck angemessene und dem Stand der Technik entsprechende Sicherheitsmaßnahmen ergriffen werden, um Informationswerte und personenbezogene Daten hinreichend zu schützen sowie die Verfügbarkeit von informations- bzw. kommunikationstechnischen Verfahren einschließlich der sie unterstützenden Systeme der IKT zu gewährleisten.

Dabei sind insbesondere:

- Prozesse zur Steuerung, Überwachung und Verbesserung der Informationssicherheit zu etablieren,
- risikoorientierte Richtlinien und Arbeitsanweisungen zu erlassen sowie deren Umsetzung und Effektivität fortlaufend zu überwachen und zu verbessern.
- Für Richtlinien und Arbeitsanweisungen gilt ab ihrer Freigabe bis zur verbindlichen Umsetzung eine Übergangsfrist von drei Monaten. Ausnahmen von dieser Vorgehensweise sind in dem jeweiligen Dokument festzuhalten.

2.2 Adressaten

Die Inhalte dieser Leitlinie sind verbindlich für das Personal der TEN (Arbeitnehmer, Mitarbeiter aus Arbeitnehmerüberlassung, Praktikanten, Werkstudenten, Auszubildende). Weiterhin sind die Inhalte verbindlich für Dritte, die:

- Geschäftsprozesse der TEN als Dienstleistung ausführen,
- an Geschäftsprozessen der TEN teilnehmen,

- auf interne, nicht öffentliche Informationen zugreifen,
- Zugang zu internen IKT-Systemen bekommen und
- Zutritt zu Räumlichkeiten mit Bezug zu Informationen oder zur Informationsverarbeitung haben.

2.3 Erfüllung des gesetzlichen Rahmens

Die Netzbetreiber sind gemäß der gesetzlich verankerten Aufgabe der ununterbrochenen Gewährleistung eines gesicherten Netzbetriebes gemäß Energiewirtschaftsgesetz (EnWG) und insbesondere durch den IT-Sicherheitskatalog der Bundesnetzagentur (BNetzA) sowie gemäß Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) und dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) dazu verpflichtet, im Hinblick auf die Ergebnisse von Risikoanalysen angemessene Maßnahmen zum Schutz der IKT zu ergreifen und diese permanent den Erfordernissen anzupassen.

Zur Steuerung der dazu notwendigen Prozesse sind ein Informationssicherheits-Managementsystem (ISMS) nach DIN ISO/IEC 27001 einzuführen, Maßnahmen nach DIN ISO/IEC 27002 und DIN EN ISO/IEC 27019 umzusetzen sowie die Wirksamkeit des ISMS durch ein Zertifikat nachzuweisen.

Zur Wahrnehmung der Meldepflicht von Sicherheitsvorfällen an das Bundesamt für Sicherheit in der Informationstechnik (BSI) gemäß § 8 b Abs. 4 BSI-Gesetz (BSIG) hat die TEN eine zentrale Kontakt- und Meldestelle einzurichten.

3 Informationssicherheit bei der TEN

3.1 Schutzziele der Informationssicherheit

Eine der Grundlagen des gesellschaftlichen Lebens in der Bundesrepublik Deutschland besteht in einer zuverlässig funktionierenden Energieversorgung. Ein länger anhaltender flächendeckender Ausfall der Energieversorgung hätte gravierende Folgen für das gesamte Gemeinwesen.

Die Basis der modernen Energieversorgung mit einer Vielzahl dezentraler Erzeugungsanlagen und Marktakteuren mit einem unterschiedlichen Rollenverständnis besteht neben dem Netz für den Energietransport in einer, den sicheren Netzbetrieb unterstützenden, intakten IKT.

Die sich verdichtende Massendatenverarbeitung stellt einerseits die Voraussetzung für die Einführung intelligenter Steuerungsalgorithmen dar, bringt andererseits aber auch Risiken mit sich, wenn die hochkomplexen Systeme der IKT geschädigt werden oder ausfallen.

Die Schutzziele zur Gewährleistung eines sicheren Netzbetriebes umfassen bei der TEN:

- **die Sicherstellung der Verfügbarkeit der zu schützenden Systeme und Daten**
  (Gewährleistung des nutzbaren und bedarfsorientierten Zugangs zu Systemen, Informationen und zugehörigen Werten für berechtigte Benutzer)
- **die Sicherstellung der Integrität der verarbeiteten Informationen und Systeme**
  (Sicherstellung der Richtigkeit und Vollständigkeit von Informationen und Verarbeitungsmethoden)
- **die Gewährleistung der Vertraulichkeit der mit den betrachteten Systemen verarbeiteten Informationen**
  (Gewährleistung des physikalischen bzw. logischen Zugangs zu Informationen nur für Zugriffsberechtigte)

3.2 Vertragliche Anforderungen an die Informationssicherheit

Zur Wahrung der Schutzziele der Informationssicherheit definiert die TEN in Dienstleistungsverträgen die Anforderungen an die Informationssicherheit bei Dienstleistern, welche Zugang zu den Werten der TEN haben. Darüber hinaus sind Vorgaben für die Überprüfung des Sicherheitsniveaus beim Dienstleister festgelegt.

Im Rahmen von Service Level Agreements (SLAs) mit Dritten vereinbart die TEN zudem Qualitätsziele und deren Einhaltung mit qualitativen und quantitativen Anforderungen bzw. Angaben (u. a. Reaktionszeiten und Verfügbarkeiten).

Bei Notwendigkeit werden entsprechende Vertraulichkeitsvereinbarungen mit Dritten abgeschlossen.

3.3 Bedeutung der IKT für den sicheren Netzbetrieb

Die TEN als 100 %-Tochtergesellschaft der Thüringer Energie AG (TEAG) betreibt Energienetze als Verteilnetzbetreiber im Bundesland Thüringen.

Insbesondere mit dem Betrieb der 110 kV-Netze und dem Gashochdrucknetz kommt ihr eine Schlüsselstellung innerhalb der Netzinfrastruktur in Thüringen zu. Der zuverlässige Betrieb der IKT als eine der wesentlichen Voraussetzungen für den sicheren Betrieb der Energienetze hat somit eine besondere Bedeutung für das Bundesland Thüringen und darüber hinaus für die vorgelagerten Netzbetreiber.

Einen sicheren Netzbetrieb zeichnet dabei aus, zu jeder Zeit die zur Gewährleistung einer ununterbrochenen Energieversorgung notwendigen Prozesse zu beobachten und zu steuern und damit einen gefahrlosen, sicheren und zuverlässigen Betrieb von Energieversorgungskomponenten, -systemen und -netzen garantieren zu können.

Zielstellung ist hierbei die Einhaltung aller physikalischen und technischen Parameter innerhalb der Normen und Verbändevereinbarungen sowie der anerkannten Regeln der Technik, um so den Anforderungen zum Schutz kritischer Infrastrukturen gerecht zu werden.

Der gesicherte Betrieb der IKT sowie der sichere Umgang mit den damit verarbeiteten Informationen haben somit bei der TEN einen überaus hohen Stellenwert und sind für das Unternehmen von existenzieller Bedeutung.

Im Rahmen der Planung von Systemen und Komponenten der IKT mit langfristiger Laufzeit berücksichtigt die TEN, soweit möglich, bereits absehbare Änderungen oder Erweiterungen von Anforderungen, sodass diese mit angemessenem Anpassungsaufwand erfüllt werden können.

3.4 ISMS

Die Beschreibung des bei der TEN etablierten Informationssicherheits-Managementsystems (ISMS) umfasst die Leitlinie, Richtlinien, Arbeitsanweisungen, Prozesse sowie weitere betriebliche Dokumentationen.
Der Aufbau des ISMS der TEN ist in **Abbildung 1** dargestellt.

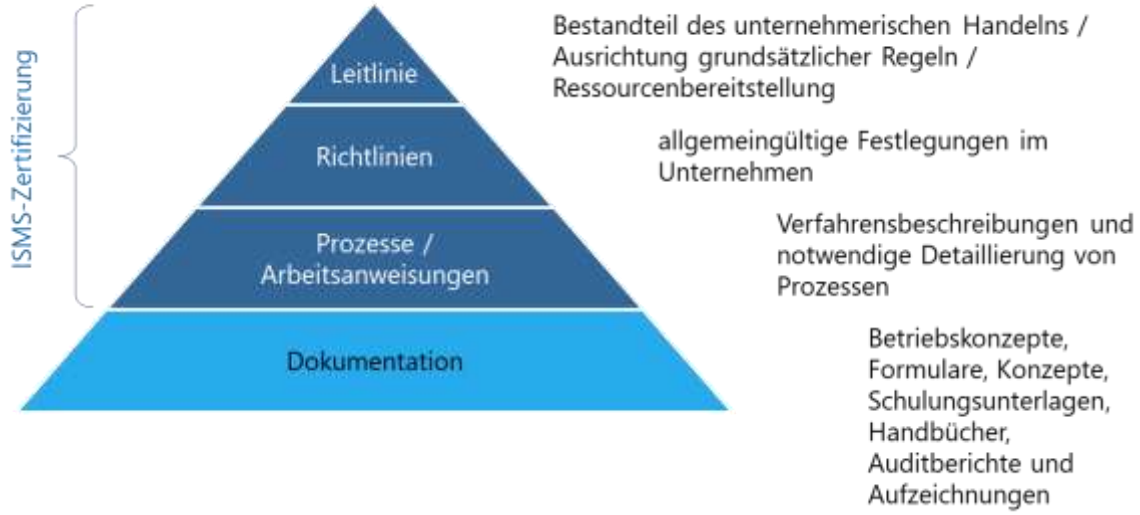

Abbildung 1: Dokumentenpyramide des ISMS der TEN

3.5 Sicherheitsmaßnahmen

Unternehmensinformationen sind ein wichtiger Vermögenswert. In digitaler wie in physischer Form müssen diese ordnungsgemäß behandelt werden, um sie vor Verlust und Diebstahl zu schützen und um sicherzustellen, dass sie dem Unternehmen jederzeit zur Verfügung stehen.

Um die Informationssicherheit für einen sicheren Netzbetrieb zu garantieren, sind die folgenden angemessenen Sicherheitsmaßnahmen notwendig:

- technische Maßnahmen (physischer Art, Hardware, Software, Konfigurationen)
- organisatorische Maßnahmen (verbindliche Regeln und Vorgaben)
- personelle Maßnahmen (Schulung, Personalmanagement)

Die Sicherheitsmaßnahmen werden in

- Richtlinien,
- Arbeitsanweisungen und
- Prozessbeschreibungen

geregelt und in

- Betriebskonzepten,
- technischen Handbüchern,
- Dokumentationen und
- Aufzeichnungen

beschrieben und nachgewiesen.

Als verbindliche Sicherheitsmaßnahmen gelten insbesondere:

- Jeder, der Informationen nutzt, ist im Rahmen der Vorgaben für deren Sicherheit verantwortlich.
- Jede schützenswerte Information ist gemäß dem erforderlichen Sicherheitsniveau zu behandeln.
- Nur eindeutig ausgewiesene Personen mit entsprechenden Berechtigungen erhalten Zugang bzw. Zugriff auf schützenswerte Informationen.
- Berechtigungen für den Zugriff auf Informationen werden nur dann vergeben, wenn es für die jeweilige Tätigkeit notwendig ist. Es werden nur die Berechtigungen vergeben, die im Rahmen der Aufgabenerfüllung benötigt werden.

- Jeder Mitarbeiter ist aufgefordert, jederzeit aktiv an der Erkennung und Vermeidung von Sicherheitsvorfällen mitzuwirken.
- Alle Systeme der IKT werden gemäß den Richtlinien und Arbeitsanweisungen genutzt.
- Soweit möglich werden personalisierte Benutzerkennungen und Passwörter benutzt, welche zweckgebunden vergeben werden.
- Der Grundsatz eines aufgeräumten Büros bzw. Schreibtisches sowie des gesperrten Bildschirms wird beachtet.

4 Organisation

4.1 Aufbau der Sicherheitsorganisation

Zur Sicherstellung der Wirksamkeit des ISMS ist eine Sicherheitsorganisation im Unternehmen etabliert, welche alle Aktivitäten zur Lenkung, Umsetzung und Verbesserung der Informations-sicherheit bei der TEN überwacht.

Folgende Gremien sind definiert:

- das Informations- und IT-Sicherheit (Gremium Management und Beauftragte)
- das Emergency Response Team (Rufbereitschaft)
- das Change Advisory Board (Änderungsberatungsausschuss)

Folgende Rollen und Verantwortlichkeiten sind definiert:

Geschäftsführung

- Gesamtverantwortung für die Informationen und IKT-Systeme des Unternehmens
- Gesamtverantwortung für die Informationssicherheit
  - Initiieren und Koordinieren des ISMS
  - Ressourcen für das ISMS zur Verfügung stellen
  - Besetzung der Rollen und Verantwortlichkeiten
  - Integration der Anforderungen des ISMS in die Geschäftsprozesse
  - Festlegung der Ziele der Informationssicherheit
  - Sorgen für Priorität und Aufmerksamkeit der/auf Informationssicherheit
  - Sicherstellung von Schulungen zur Informationssicherheit
  - organisatorische Verankerung von Aktivitäten zur Etablierung, Erhaltung und Weiterentwicklung des ISMS
  - angemessene Einbettung des ISMS in die Strukturen und Hierarchien

IS-Beauftragter

- Umsetzung der Ziele der Informationssicherheit
- Anleitung IT-Koordinatoren und IT-Sicherheitsbeauftragte
- Berichtspflicht an die Geschäftsführung

Organisation des ISMS

- Etablierung, Erhaltung, kontinuierliche Verbesserung und Weiterentwicklung des ISMS
- Integration des ISMS in die Geschäftsprozesse und entsprechende Kontrolle
- Auditmanagement (zentrale Zertifizierungsstelle gemäß Vorstandsbeschluss 66/2014)

IT-Sicherheitsbeauftragter
- Umsetzung von Maßnahmen der Informationssicherheit bzw. des ISMS
- Umsetzung von Maßnahmen zur IT-Sicherheit der IKT des Netzbetriebes

Ansprechpartner IT-Sicherheit gegenüber der BNetzA (APITS)
- Wahrnehmung der Auskunftspflicht gegenüber der BNetzA gemäß IT-Sicherheitskatalog
- Sicherstellung der Anbindung des Netzbetreibers an relevante Kommunikationsinfrastrukturen für Lageberichte und Warnmeldungen sowie zur Bewältigung großflächiger IKT-Krisen

Führungskräfte (Bereichs- und Fachgebietsleiter)
- Übernahme der Verantwortung für die Informationen und IKT-Systeme in ihrem Verantwortungsbereich
- Umsetzung der Anforderungen des ISMS im Rahmen der Mitarbeiterführung

IT-Administratoren und IT-Koordinatoren (eigene und externe)
- Umsetzung der festgesetzten Maßnahmen des ISMS

Verantwortliche Personalmanagement
- Sicherstellung der Umsetzung von personellen Maßnahmen und Schaffung der Voraussetzungen

Verantwortliche Facility Management
- Sicherstellung der Umsetzung aller Maßnahmen und Schaffung der Voraussetzungen für Verwaltungsstandorte

Mitarbeiter
- Einhaltung der Vorgaben zur Informationssicherheit über ihr entsprechendes Verhalten im Arbeitsumfeld

Meldestelle
- Innerhalb der Organisation wird eine zentrale Stelle zur Erfassung von Sicherheitsvorfällen eingerichtet. Diese ist sowohl für Mitarbeiter als auch für Externe erreichbar und dient als Kontakt- und Meldestelle gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI), wie sie gemäß Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV) sowie nach § 8 b Abs. 4 BSIG gefordert wird.

4.2 Unterweisungs- und Sensibilisierungsmaßnahmen

Über die dargestellten Rollen hinaus ist es für die Wirksamkeit des ISMS notwendig, dass alle Führungskräfte, Mitarbeiter und Lieferanten die für sie zutreffenden Informationssicherheitsregelungen kennen und beachten.

Um dies sicherzustellen, erfolgt für die Mitarbeiter der TEN regelmäßig eine Unterweisung über die Vorgaben des ISMS. Die Wirksamkeit dieser Unterweisungen wird im Rahmen von Audits/Reviews sowie selektiv durch die Erhebung von Kennzahlen überprüft.

Lieferanten werden über die Anforderungen des ISMS der TEN im Rahmen der vertraglichen Vereinbarungen in Kenntnis gesetzt. Die Überprüfung des vereinbarten Sicherheitsniveaus erfolgt durch regelmäßige Audits/Reviews.

4.3 Sanktionen

Für die Einhaltung der in dieser Leitlinie definierten Rahmenbedingungen, Regeln und Vorgaben zur Informationssicherheit sind neben den Mitarbeitern (Nutzer/Anwender) auch deren Vorgesetzte verantwortlich.

Die Regelungen dieser Leitlinie entfalten im Arbeitsverhältnis direkte Wirkung. Die Nichtbeachtung ihrer Inhalte kann damit arbeits- oder sonstige zivil- und/oder strafrechtliche Konsequenzen haben.

5 Kontinuierlicher Verbesserungsprozess

Durch eine kontinuierliche Verbesserung der Regelungen und deren Einhaltung mittels jährlicher interner Audits wird das angestrebte Informations- bzw. IKT-Sicherheitsniveau sichergestellt. Abweichungen sollen mit dem Ziel analysiert werden, die Sicherheitssituation zu verbessern und ständig auf dem aktuellen Stand zu halten. Im Rahmen eines kontinuierlichen Verbesserungsprozesses unterliegt die vorliegende Leitlinie einer regelmäßigen Verbesserung und Aktualisierung.

Das bedeutet insbesondere:

- regelmäßige Überprüfung von Einhaltung, Aktualität und Wirksamkeit der Leitlinie
- zwingende Überprüfung der Leitlinie nach Veränderungen der Bedrohungslagen, Änderungen von Technologien, aktuellen Ereignissen, gesetzlichen und normativen Änderungen
- mindestens jährliche Überprüfung (z. B. im Rahmen eines internen Audits)

6 Versionsverwaltung

Version	Datum	Änderung	Name/OE
V 1.0	16.09.2016	Ersterstellung	ISMS-Team
V 2.0	20.09.2016	Weiterbearbeitung/Anpassung	Schulz BF Fa. ASC
V 3.0	18.10.2016	Finalisierung	ISMS-Team
V 4.0	18.10.2017	Überarbeitung nach externem Audit Stufe 1	Schulz BF Fa. ASC
V 4.1	18.10.2019	Review durchgeführt – keine Überarbeitung notwendig	Oelze BF Heß BF
V 4.2	15.07.2020	Review durchgeführt – keine Überarbeitung notwendig	Oelze BF Heß BF
V 5.0	28.09.2021	Überarbeitung	Tille GFB Dr. Agsten BF Heß BF
V 6.0	11.10.2022	Überarbeitung	Dr. Agsten BF