ISMS-Leitlinie

für die

Energieversorgung Gera GmbH

GeraNetz GmbH

1. Inhaltsverzeichnis

2. Dokumentenlenkung

2.1 Historie / Versionsübersicht

2.2 Freigabeelemente

2.3 Geltungsbereich und -Ausschlüsse

Die Leitlinie wird auf das gesamte Informationssicherheitsmanagement (kurz: ISMS), Prozesse, Verfahren und Pläne sowie sonstige Dokumentationen angewendet.
Die Informationssicherheitsleitlinie hat für alle Mitarbeiter des Unternehmens Gültigkeit sowie für externe Dienstleister oder Servicekräfte die mit Daten, Informationen und dem IKT-System (IKT=Informations- und Kommunikationstechnik) der EGG und der GNG in Berührung kommen. Die Gewährleistung der Informationssicherheit ist nur sichergestellt, wenn alle Anwender (interne / externe Mitarbeiter) diese definierte Informations-Sicherheit kennen und dementsprechend verantwortungsvoll handeln.

2.4 Geltungszeit

Dieses Dokument gilt vom 01.08.2018 unbefristet.

2.5 Revisionsdatum

Zum 01.08.2019 ist das Dokument erstmalig einer Revision im Rahmen der Dokumentenlenkung zu unterziehen, darauffolgend mindestens einmal jährlich oder auf Grund von Veränderungen im Prozess.

2.6 Klassifikation

Für dieses Dokument gilt die Datenklassifikation „öffentlich“.

3. Allgemeines

3.1 Zweck

Für Energieversorgungsunternehmen steht die Gewährleistung des sicheren Netzbetriebes und die Versorgungssicherheit ihrer Kunden mit Strom, Gas, Wärme, Kälte sowie IKT-Infrastrukturen (IKT – Informations- und Kommunikationstechnologie) im Vordergrund. Um diese gewährleisten zu können, ist die Informationstechnik (kurz: IT) durch zunehmende Digitalisierung, Komplexität und erhöhten technischen Anforderungen eine primäre Komponente. Die ISMS-Leitlinie definiert die geforderten Informations- und IT-Sicherheitsziele und die damit verbundenen Informations-Sicherheitsstrategien, die zum Erfolg des Unternehmens entscheidend beitragen.

Die Einhaltung dieser Leitlinie ist verpflichtend vor dem Hintergrund der steigenden Vernetzung, einhergehend mit einer steigenden Bedrohungslage. Sie dient der Gewährleistung eines sicheren Netzbetriebes.

Die Geschäftsführung ist für die Organisation der Sicherheit des Unternehmens verantwortlich und hält die erforderlichen Maßnahmen für die Gewährleistung der Verfügbarkeit, Vertraulichkeit und Integrität von Daten, Informationen, Dokumenten, Anwendungen, IT-Systemen und Infrastrukturen in dieser Informations-Sicherheitsleitlinie fest.

Die Geschäftsführung beeinflusst durch ihre Akzeptanz und Unterstützung maßgeblich den Erfolg der Informationssicherheit im Unternehmen. Jeder Mitarbeiter ist verpflichtet, sich nach innen und außen an diese Leitlinie zu halten.

In dieser Leitlinie wird der Informations-Sicherheitsprozess beschrieben. Sie ist somit ein übergeordneter Bestandteil der Richtlinie „IT-Sicherheit“.

4. Stellenwert

Grundlage des sicheren Netzbetriebes sind IKT-Systeme. Ihr störungsfreier Betrieb ist sicherzustellen. Mit dem von der BNetzA veröffentlichten Sicherheitskatalog in der jeweils gültigen Fassung ergeben sich Anforderungen, die die vorliegende Leitlinie berücksichtigt und umsetzt. Alle weiteren gesetzlichen Forderungen und die für die Unternehmen gültigen Geschäftsanweisungen werden beachtet.

5. Zielsetzung

Die Informationssicherheit ist ein integraler Bestandteil aller Geschäftsprozesse. Die Definition der Informationssicherheit und deren Umsetzung in allen Geschäftsprozessen besitzt in den Unternehmen höchste Priorität und ist wie folgt definiert:

Die Informationssicherheit hat jederzeit die Verfügbarkeit, Vertraulichkeit und Integrität aller Informationen in unseren Unternehmen zu gewährleisten. Unter Informationen versteht man Daten (Datenbanken, Dokumente), IT-basierende Geschäftsprozesse (Kommunikation, Datenaustausch, Transaktionen) und Infrastrukturen (Räumlichkeiten, Netzwerke, Komponenten). Geltende Gesetze, Regelungen und Verträge sind einzuhalten, der Datenschutz ist zu gewährleisten und die Rechte der Mitarbeiter sind zu schützen.

- Verfügbarkeit: Der Zugang zu Informationen muss jederzeit für die berechtigten Personen möglich sein.
- Vertraulichkeit: Es wird gewährleistet, dass nur Zugriffsberechtigte einen physikalischen bzw. logischen Zugang zu Informationen haben.
- Integrität: Es wird sichergestellt, dass die Informationen jederzeit vollständig, vertrauenswürdig, richtig und aktuell gepflegt sind.

Im Rahmen des ISMS werden alle auf die Ziele wirkenden Risiken identifiziert und bewertet.

Wir definieren und implementieren passende organisatorische und technische Strategien und Maßnahmen für den Umgang mit den Risiken. Nach Abstimmung mit dem verantwortlichen Personenkreis / Rollen sind diese an geeigneter Stelle zu dokumentieren und dem verantwortlichen Personenkreis zur Verfügung zu stellen.

6. Prinzipien der Informations-Sicherheitsstrategie

Die Anwender (interne / externe Mitarbeiter) sind über die Informationssicherheit in den Unternehmen unterrichtet, besitzen ein Grundverständnis und werden regelmäßig belehrt und informiert.

Die Anwender haben sich ausschließlich in ihrem Zuständigkeitsbereich zu bewegen, Ausnahmeregelungen, Berechtigungen und Zugriffsrechte werden begründet und dokumentiert.

Der Betrieb aller IT-Systeme erfolgt in sicheren, überwachten und abgeschlossenen Umgebungen. Daten- und Backup-Server sollten räumlich getrennt und redundant sein.

Regelmäßig sind Datensicherungen durchzuführen, dies gilt auch für mobile Geräte (Datenträger, Smartphones und Notebooks). Die erstellten Backups sind regelmäßig auf ihre

Funktionalität zu überprüfen und die Speichermedien sind an einem sicheren Ort zu verwahren.

Vor unberechtigten Zugriffen sind die Informationen zu schützen.

IT-Systeme sind immer auf dem aktuellen Versionsniveau zu pflegen und das Erfordernis von Updates / Upgrades ist stets zu prüfen.

IT-Systeme sind vor Schadsoftware zu schützen.

Die Arbeit der Administratoren an den IT-Systemen muss nachvollziehbar und transparent sein. Service-Level-Agreements (SLA) sind zu definieren und einzuhalten.

Die Betreuung der IT-Systeme erfolgt langfristig durch kompetentes und geschultes Fachpersonal.

Eine regelmäßige Überprüfung und Dokumentation der Wirksamkeit und Funktionsfähigkeit von Schutzmaßnahmen ist erforderlich.

Bei Ereignissen und Vorfällen in der Informationssicherheit sind unverzüglich der ISMS-B, der ITSiBe sowie die IT-Verantwortlichen zu informieren. Diese werden revisionssicher dokumentiert und stets kommuniziert.

Ansprechpartner für ausgewiesene Belange sind bekannt zu geben und deren Erreichbarkeit zu jeder Zeit bzw. über Vertreter- oder Bereitschaftsregelungen zu gewährleisten, um alle Geschäftsprozesse aufrecht zu erhalten.

Die Abstimmung zwischen Geschäfts- und ISMS/IT-Strategie hat regelmäßig zu erfolgen.

7. Organisation und Verantwortlichkeiten

Die Geschäftsführung der Energieversorgung Gera GmbH und der GeraNetz GmbH trägt die Gesamtverantwortung für die Informationssicherheit im jeweiligen Unternehmen und legt die Beteiligten am Informationssicherheitsprozess fest. Zur Erreichung der Informationssicherheitsziele werden durch die Geschäftsführung ausreichend finanzielle Mittel und Ressourcen zur Verfügung gestellt.

Die Umsetzung und Einhaltung der Leitlinie wird von den Geschäftsführungen der Unternehmen als letzte Kontrollinstanz verantwortet.

Gemäß dem IT-Sicherheitskatalog der BNetzA wurde ein Ansprechpartner Informationssicherheit benannt.

Beteiligte am Informationssicherheitsprozess

(1) Zentrales IT-Leitmanagement (ITLM)
(2) IT-Sicherheitsbeauftragter (ITSiBe)
(3) ISMS-Beauftragter (ISMS-B)
(4) Ansprechpartner IT-Sicherheit (APITS) gegenüber der BNetzA
(5) Datenschutzbeauftragter (DSB)

(6) Gleichbehandlungsbeauftragter
(7) IT-Verantwortlicher und Dienstleister
(8) Externe Dienstleister
(9) Anwender und Mitarbeiter

(1) Zentrales IT-Leitmanagement
Ein firmeninternes IT-Leitmanagement (kurz: ITLM) als Koordinierungsausschuss ist aufzubauen, welches den ISMS-Beauftragten und den IT-Sicherheitsbeauftragten unterstützt. Es besteht aus Vertretern der IT-Abteilung, kaufm. und techn. Bereichen, Management und dem Betriebsrat. Die Vertreter haben die Funktion von dezentralen Beauftragten für Informationssicherheit. In diesem Managementteam werden grundlegende strategische Abstimmungen getroffen, Änderungen besprochen, Geschäftsprozesse optimiert, Synergieeffekte ermittelt und umgesetzt.

(2) IT-Sicherheitsbeauftragter
Ein IT-Sicherheitsbeauftragter (kurz: ITSiBe) ist zu benennen bzw. zu bestellen. Er ist federführend für die strategische Ausrichtung der IT-Sicherheit zuständig. Ein jährlicher IT-Sicherheitsbericht ist den Geschäftsführungen vorzulegen.

(3) ISMS-Beauftragter
Ein ISMS-Beauftragter (kurz: ISMS-B) ist zu benennen bzw. zu bestellen. Der ISMS-B ist verantwortlich für die Überwachung des ISMS-Prozesses und gegebenenfalls erforderliche Prozessanpassungen. Mindestens einmal jährlich ist den Geschäftsführungen ein Bericht zur Risikoeinschätzung vorzulegen.

(4) Ansprechpartner IT-Sicherheit gegenüber der BNetzA
Der Ansprechpartner IT-Sicherheit (kurz: APITS) ist zu bestellen und der BNetzA verpflichtend zu melden. Der APITS muss der BNetzA zu nachfolgenden Punkten unverzüglich Auskunft geben können:

- Zum Umsetzungsstand der Anforderungen des IT-Sicherheitskataloges.
- Zu aufgetretenen Sicherheitsvorfällen sowie der Art und des Umfangs etwaiger hierdurch hervorgerufener Auswirkungen.
- Zur Ursache aufgetretener Sicherheitsvorfälle sowie zu Maßnahmen zu deren Behebung und zukünftigen Vermeidung.

(5) Datenschutzbeauftragter
Ein Datenschutzbeauftragter (kurz: DSB) ist zu bestellen. Der DSB wirkt auf die Einhaltung der DSGVO und des BDSG und anderer Vorschriften zum Datenschutz im Unternehmen hin. Die Kontrollkompetenz erstreckt sich auf das gesamte Unternehmen. Er besitzt Weisungsfreiheit bei der Ausübung seiner Tätigkeit auf dem Gebiet des Datenschutzes. Die Datenschutzorganisation des Unternehmens mit den benannten Bereichsdatenschutzkoordinatoren unterstützt den DSB in der Ausübung seiner Tätigkeit.

(6) Gleichbehandlungsbeauftragter
Der/die Gleichbehandlungsbeauftragte ist zu bestellen, in die Belange der Informationssicherheit einzubeziehen und zur Verschwiegenheit schriftlich verpflichtet.

(7) IT-Verantwortlichen und Dienstleister
Die IT-Verantwortlichen und Dienstleister sind für die Realisierung der Informationssicherheitsrichtlinie und deren Konzepte sowie für die technischen Richtlinien

verantwortlich. Sie haben diese fortzuführen, weiterzuentwickeln und zu dokumentieren. Außerdem sind sie erster Ansprechpartner für die IT gegenüber Mitarbeitern und Kunden.

(8) Externe Dienstleister
Externe Dienstleister oder Auftragnehmer im Bereich der IT werden über die Iinformations-Sicherheit belehrt und haben sich zur Einhaltung schriftlich zu verpflichten.

(9) Anwender und Mitarbeiter
Die Anwender (Mitarbeiter) tragen die Verantwortung für die sachgerechte Benutzung des IT-Systems und aller Informationen. Jeder Anwender (Mitarbeiter) hat die Pflicht, Vorfälle im Zusammenhang mit der Informationssicherheit zu melden (z.B. Datenverlust oder Verlust von vertraulichen Dokumenten).

8. Beschreibung des Informationssicherheitsprozesses

Ein Informationssicherheitsprozess besteht grundlegend aus drei Ebenen, die aufeinander aufbauen und abhängig voneinander wirken.

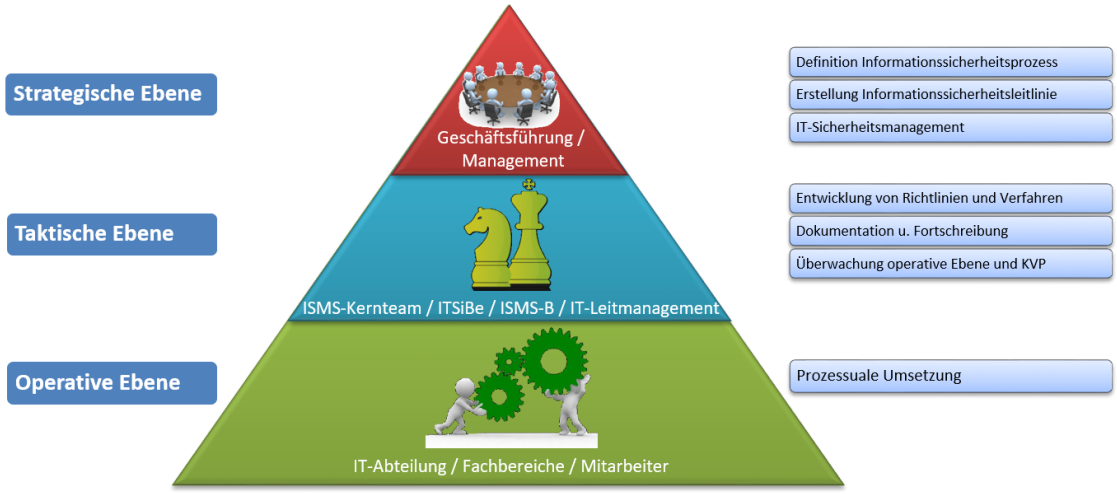

Abbildung 1: Der Informationssicherheitsprozess

1. Strategische Ebene

   Durch die Geschäftsführung bzw. das Management werden der Informationssicherheitsprozess, die Informationssicherheitsleitlinie und die Informationssicherheitsziele im Unternehmen definiert.

2. Taktische Ebene

   IT-Leitmanagement, ISMS-Kernteam, ISMS-Beauftragter und IT-Sicherheitsbeauftragter sind verantwortlich für die Wirksamkeit der Informationssicherheitsrichtlinie und für die damit verbundenen Informationssicherheitskonzepte, definiert in Richtlinien, Verfahren, Dokumentationen und Formularen. Sie haben die operative Ebene und die Umsetzung des

kontinuierlichen Verbesserungsprozesses (kurz: KVP) zu überwachen bzw. selbst aktiv zu betreiben.

3. Operative Ebene

   Informationssicherheitskonzepte werden realisiert und technische Richtlinien durch die Mitarbeiter, IT-Abteilung und die technischen Bereiche entwickelt.

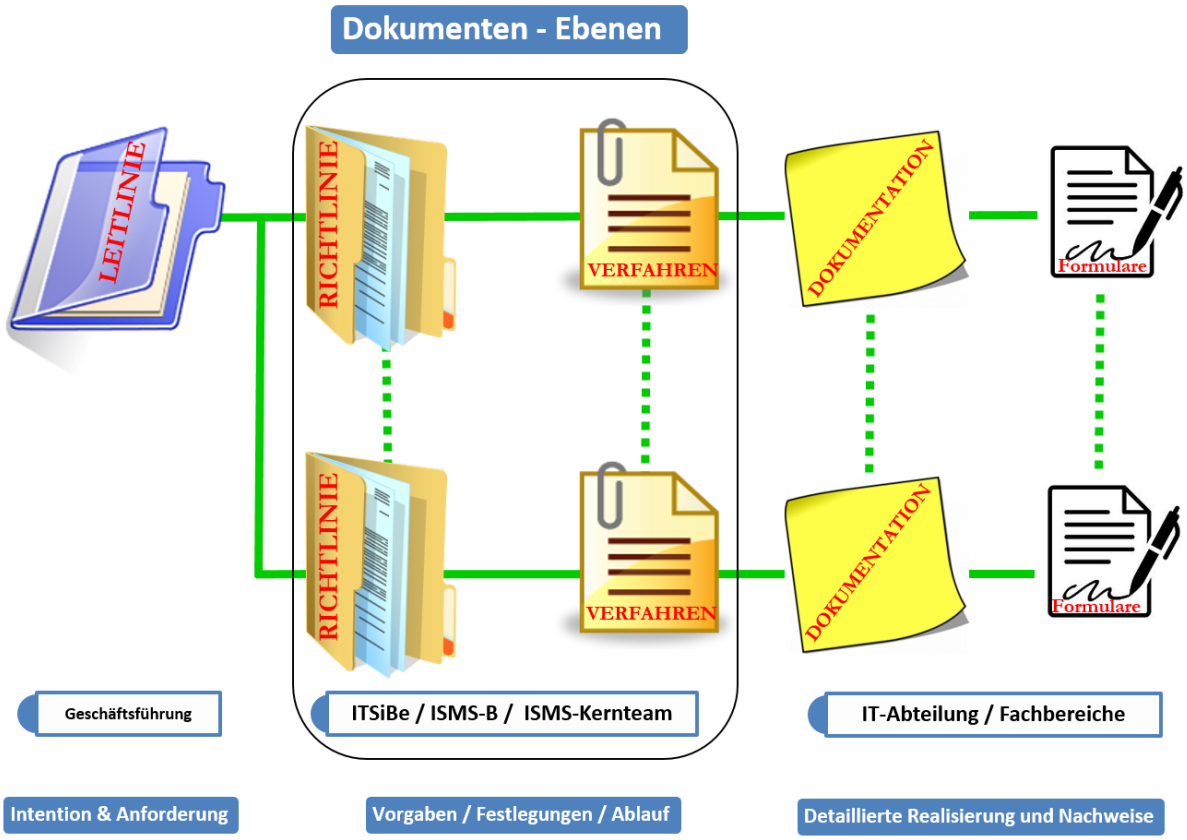

Abbildung 2: Dokumentation des Informationssicherheitsprozesses

9. Umsetzung und Kontinuität

Die Umsetzung der Informationssicherheitsleitlinie im Rahmen einer Informationssicherheitsrichtlinie erfolgt in der operativen Ebene und wird regelmäßig vom IT-Leitmanagement und dem IT-Sicherheitsbeauftragten überprüft.

Die fortlaufende Verbesserung ist ein wichtiger Bestandteil des ISMS. In regelmäßigen Abständen wird die Wirksamkeit des ISMS überprüft, bewertet und optimiert.

Jeder Mitarbeiter ist für die Gewährleistung der Informationssicherheit im Unternehmen zuständig, für sein Handeln verantwortlich sowie angehalten, eigenverantwortlich und stetig Verbesserungsvorschläge für das ISMS in Erwägung zu ziehen und gegenüber dem ISMS-Beauftragten zu kommunizieren. Hierunter können organisatorische (z.B. Schwierigkeiten bei

der Ausführung gegebener Verfahren) als auch technische Maßnahmen (z.B. Einsatz neuer Technologien) zählen.

Die Kenntnisnahme der Informationssicherheitsleitlinie wird von diesen bestätigt und turnusmäßig aktenkundig belehrt.

9.1 Aktualisierung, Überprüfung und Verbesserung

Die Informationssicherheitsleitlinie sowie die daraus abgeleitete IT-Sicherheitsrichtlinie sind mindestens einmal jährlich durch das IT-Leitmanagement auf Aktualität zu überprüfen. Über Neuerungen oder grundlegende Veränderungen sind die Anwender (Mitarbeiter) zu informieren.

10. Schulungsmaßnahmen

Wir stellen sicher, dass alle Mitarbeiter, die im Rahmen des ISMS Tätigkeiten durchführen, regelmäßig geschult und unterwiesen sind. Hierfür dienen geeignete Schulungspläne.

Die Mitarbeiter sind regelmäßig zum Thema Informationssicherheit zu sensibilisieren.

11. Verstöße und Sanktionen

Bei einem Verstoß bzw. bei Nichteinhaltung der ISMS-Leitlinie bedarf es zielführender Konsequenzen. Nach geltenden Regelungen oder gesetzlichen Bestimmungen können die Verstöße geahndet werden. Es ist besonders wichtig, Verstöße zu kommunizieren, um daraus zu lernen und alle Mitarbeiter zu sensibilisieren.

12. Referenzdokumente

- Datenschutz- und Datensicherheitsrichtlinie