Informationssicherheitspolitik

Rahmenbedingungen, Strategien und Ziele

Stadtwerke Suhl/Zella-Mehlis Netz GmbH

Änderungshistorie

Version	Autor	Datum	Beschreibung
0.1	secopan	30.05.2016	Neuerstellung
1.0	Erik Könitzer (EK)	22.08.2016	Layout-/Formulierungsanpassungen SWSZ
2.0	EK	26.01.2018	Inhaltliche Überarbeitung, Prüfung Ist-/Sollzustand
2.1	EK	03.01.2019	Revision
3.0	EK	30.12.2019	Revision und komplette inhaltliche Überarbeitung
3.1	D. Lichtleitner	24.11.2020	Anpassungen Dokumentenlenkung
3.2	EK	24.11.2020	Revision
4.0	GF SWSZ/Netz	15.12.2020	Freigabe
4.1	EK	23.01.2023	Revision und inhaltliche Überarbeitung
5.0	GF SWSZ/Netz	30.01.2023	Freigabe
5.0	EK	19.01.2024	Revision, Ergänzung ISMS-Koordinator Netz
6.0	EK	22.01.2025	Komplette inhaltliche Überarbeitung Normumstellung ISO 27001:2017 auf 2022
6.0	GF Netz	11.02.2025	Freigabe

Inhalt

1. Ziel und Geltungsbereich 4
2. Stellenwert der Informationssicherheit 4
3. Schutzziele und Rahmenbedingungen 4
   3.1. Kernelemente der Sicherheitsstrategie 5
   3.2. Sicherheitsmaßnahmen durch Richtlinien, Festlegungen und Prozesse 5
   3.3. Adressaten 6
4. Organisationsstruktur 6
5. Verantwortung der Mitarbeiter und Dienstleister 7
6. Unterstützende Richtlinien und Anweisungen 7
7. Kontinuierlicher Verbesserungsprozess 8
8. Allgemeine Festlegungen 8

1. Ziel und Geltungsbereich

Ziel der Informationssicherheit ist es, den Geschäftsbetrieb der SWSZ Netz GmbH sicherzustellen und das Risiko eines Schadens durch die Verhütung von Sicherheitsvorfällen und die Reduzierung ihrer potenziellen Auswirkungen zu minimieren.

Ziel ist es weiterhin, Informationen gegen alle internen, externen, absichtlichen oder versehentlichen Bedrohungen zu schützen. Aus diesem Grund hat die SWSZ Netz GmbH ein Informationssicherheitsmanagementsystem (ISMS) etabliert, welches regelmäßig auf Wirksamkeit und Angemessenheit überprüft wird.

Nach dem EnWG ist der Netzbetreiber dazu verpflichtet, ein sicheres zuverlässiges und leistungsfähiges Energieversorgungsnetz zu betreiben.

Die Gesamtverantwortung für die Informationssicherheitspolitik obliegt der Geschäftsleitung der SWSZ Netz GmbH.

Daten und Informationen werden in nahezu allen Bereichen der Unternehmen elektronisch verarbeitet, gespeichert und übermittelt. Informationstechnik spielt in allen Abteilungen sowie in der Kommunikation mit Kunden, Geschäftspartnern und anderen Organisationen eine tragende Rolle.

Demzufolge gilt diese Informationssicherheitspolitik für alle Abteilungen der SWSZ Netz GmbH und ist unter Berücksichtigung der Normen DIN EN ISO/IEC 27001, DIN EN ISO/IEC 27019 und des IT-Sicherheitskataloges gem. §11 Abs. 1a EnWG aufgestellt worden.

2. Stellenwert der Informationssicherheit

Die erfolgreiche Planung, Implementierung und Betreuung von IT-Infrastrukturen, Kommunikations- und Betriebstechnik impliziert einen schnellen, sicheren und aktuellen Zugriff auf Informationen, von welchen die Sicherstellung des täglichen Geschäftsbetriebs im Unternehmen abhängt.

Ein Missbrauch dieser Informationen schadet nicht nur dem Ansehen und der Reputation, sondern kann auch rechtliche Folgen und Schadensersatzansprüche verursachen. Demzufolge ist dieser Missbrauch zu verhindern.

Eine funktionsfähige Informationstechnik und ein sicherheitsbewusster Umgang mit ihr sind wesentliche Voraussetzungen für die Sicherstellung der täglichen Arbeitsabläufe und das Vertrauen unserer Kunden und Geschäftspartner.

3. Schutzziele und Rahmenbedingungen

Die Schutzziele hinsichtlich der Sicherstellung sämtlicher Geschäftsprozesse zur Gewährleistung des sicheren Strom- und Gasnetzbetriebs sind definiert und umfassen

- den Schutz von Informationen und informationsverarbeitenden Systemen gegen alle nicht autorisierten Zugriffe,

- die Gewährleistung der Vertraulichkeit und Integrität von Informationen,
- die Sicherstellung der Verfügbarkeit von Informationen und informationsverarbeitenden Systemen im operativen Geschäftsbetrieb.

3.1. Kernelemente der Sicherheitsstrategie

Zur Erreichung der Schutzziele gehören folgende Aspekte zu den Kernelementen der Sicherheitsstrategie:

- Schutz von Informationen gegen alle nicht autorisierten Zugriffe,
- Gewährleisten der Vertraulichkeit der Informationen,
- Gewährleisten der Integrität von Informationen,
- Gewährleisten der Verfügbarkeit von Informationen,
- Erfüllen von legislativen und behördlichen Auflagen mit Relevanz für die Informationssicherheit,
- Entwickeln, Verwalten und Testen von Notfallplänen,
- Anbieten und Durchführen von Informationssicherheitsschulungen für alle MA,
- Melden von Informationssicherheitsereignissen an das ISMS-Team,
- Untersuchen von Informationssicherheitsereignissen und -vorfällen durch das ISMS-Team,
- Melden von Datenschutzverletzungen an den Datenschutzbeauftragten.

3.2. Sicherheitsmaßnahmen durch Richtlinien, Festlegungen und Prozesse

Die Existenz, Sicherheit und Reputation der SWSZ Netz GmbH ist in wesentlichem Maße vom verantwortungsvollen und kompetenten Umgang mit schützenswerten Informationen sowie des fehlerfreien Betriebs informationstechnischer Systeme abhängig.

Durch interne und externe Einflüsse sind Informationen und informationsverarbeitende Systeme besonders gefährdet. Unsachgemäße Nutzung sowie bewusster und unbewusster Missbrauch erhöhen nicht nur das Gefährdungspotential, sondern verursachen bei Eintritt von Sicherheitsereignissen und -vorfällen erhebliche Mehrkosten.

Mitarbeiter sowie externe Auftragnehmer müssen sich ihrer Verantwortung im Bereich der Informationssicherheit, ihres Beitrags zur Wirksamkeit des ISMS und den Folgen bei Nichtbeachtung der Anforderungen bewusst sein, die Sicherheitsziele kennen, die Sicherheitsmaßnahmen verstehen, akzeptieren und umsetzen.

Alle Richt- bzw. Leitlinien, Vorschriften, Organisationsstrukturen sowie verbindliche Verfahrens- und Arbeitsanweisungen werden an geeigneter Stelle publiziert.

Gesetzliche Anforderungen, insbesondere die der EU-DSGVO sowie behördliche und vertragliche Anforderungen sind von allen Mitarbeitenden sowie externen Auftragnehmern einzuhalten.

Die Sicherstellung der Informationssicherheit erfolgt durch angemessene

- technische (z. B. Ertüchtigung der IT-Unternehmensumgebung),
- organisatorische (z. B. Richtlinien, Festlegungen und Maßnahmen) und
- personelle Maßnahmen (z. B. Schulungen, Personalsicherheit).

Festlegungen, Verfahrensanweisungen, Maßnahmen und Prozesse hierzu werden in der ISMS-Dokumentation, in Organisationshandbüchern, in der IT-Betriebsdokumentation sowie in Betriebsmappen detailliert beschrieben.

Nachfolgende Sicherheitsmaßnahmen sind generell zu beachten:

- für die Sicherheit der Informationen ist der jeweilige Eigner verantwortlich
- schützenswerte Informationen sind gemäß ihrer Klassifizierung zu behandeln
- der Zugang zu bzw. der Zugriff auf Informationen oder informationsverarbeitende(n) Systeme(n) ist streng reglementiert und nur möglich, wenn es zur Erfüllung dienstlicher Aufgaben notwendig ist
- jeder Mitarbeiter oder externe Auftragnehmer ist verpflichtet, seinen aktiven Beitrag zur Erkennung und Vermeidung von Sicherheitsvorfällen zu leisten
- informationsverarbeitende Systeme sind ausschließlich im Kontext der entsprechenden Richtlinien mit personalisierten Zugängen zu benutzen

3.3. Adressaten

Die Informationssicherheitspolitik gilt im Anwendungsbereich des ISMS als Handlungsanweisung für alle Mitarbeiter sowie für Dritte, die

- an Geschäftsprozessen der SWSZ Netz GmbH beteiligt sind,
- als Dienstleister für die SWSZ Netz GmbH tätig sind,
- auf als intern klassifizierte Informationen zugreifen,
- Zugang zu internen informationsverarbeitenden Systemen erhalten,
- Zutritt zu Bereichen mit erhöhtem Schutzbedarf haben.

4. Organisationsstruktur

Zur Erreichung der Sicherheitsziele wurde seitens der Geschäftsleitung ein Informationssicherheits-beauftragter (ISB) bestellt. Der ISB ist für die Erstellung und Fortschreibung des Sicherheitskonzepts sowie die Aufrechterhaltung des Sicherheitsniveaus verantwortlich. Er berichtet in seiner Funktion direkt der Geschäftsleitung.

Dem ISB werden von der Geschäftsleitung ausreichende finanzielle und zeitliche Ressourcen für die Ausübung seiner Tätigkeit zur Verfügung gestellt.

Der ISB ist durch die Geschäftsleitung sowie durch die Mitarbeiter ausreichend zu unterstützen und frühzeitig in alle Projekte einzubinden, um schon in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen.

Der ISB ist gegenüber den Mitarbeiterinnen und Mitarbeitern in Bezug auf die Aspekte der Informationssicherheit weisungsbefugt.

Der ISB ist verantwortlich für:

- die Eskalation etwaiger Risiken an die Geschäftsleitung,
- die Beratung der Mitarbeiter zu Fragen zur Informationssicherheit,
- die Schulung der Mitarbeiter in Bezug auf die Informationssicherheit.

Das ISMS-Team besteht aus:

- der Geschäftsleitung
- dem Informationssicherheitsbeauftragten,
- dem ISMS-Koordinator der SWSZ Netz GmbH
- den fachlich oder temporär zugeordneten Mitarbeitern sowie
- der Datenschutzbeauftragten.

5. Verantwortung der Mitarbeiter und Dienstleister

Jeder Mitarbeiter und Dienstleister, welcher im Auftrag der SWSZ Netz GmbH tätig ist oder tätig wird, verpflichtet sich, sorgfältig mit den ihm zur Verfügung stehenden Informationen umzugehen und die Leit- bzw. Richtlinien einzuhalten.

Eine grobfahrlässige Verletzung der Informationssicherheit kann zu disziplinarischen oder arbeitsrechtlichen Konsequenzen, straf- und zivilrechtlichen Verfahren oder Haftungs- und Regressforderungen führen.

Als grobfahrlässige Verletzungen bzw. Handlungen gelten:

- eine Kompromittierung der Reputation des Unternehmens,
- eine Bedrohung für die Sicherheit der Mitarbeiter und Dienstleister sowie des Vermögens des Unternehmens,
- die Gefährdung der Sicherheit von Informationen hinsichtlich deren Verfügbarkeit, Integrität und Vertraulichkeit,
- die Kompromittierung der Sicherheit von Daten oder Geschäftsinformationen des Unternehmens, welche zu einem tatsächlichen oder potenziellen finanziellen Verlust führt,
- der unberechtigte Zugriff auf Informationen, deren Preisgabe und/oder Änderung,
- die Nutzung von Unternehmensinformationen für illegale Zwecke.

Die grundlegenden Bestimmungen zum Maßregelungsprozess sind für die Mitarbeiter transparent in der Mitarbeiterrichtlinie dokumentiert.

6. Unterstützende Richtlinien und Anweisungen

Das ISMS umfasst neben dieser Politik weitere, verbindliche Richtlinien, Verfahrensanweisungen, Prozesse und Dokumentationen. Diese sind an geeigneter Stelle für alle Adressaten publiziert.

Sofern erforderlich, ist bei Schriftverkehr mit externen Dienstleistern, Geschäftspartnern oder Institutionen auf die im Internet unter

- swsz-netz.de → Unternehmen → Zertifizierungen → Zertifizierungen Informationssicherheit

veröffentlichten Informationssicherheitspolitik hinzuweisen.

Die freigegebenen und veröffentlichen Fassungen sind die gültigen und verbindlichen Fassungen. Druckversionen dienen lediglich der Information.

Gesetzliche und vertragliche Anforderungen, insbesondere die der DSGVO, sowie die speziellen Festlegungen der Organisationshandbücher sind von allen Mitarbeitern einzuhalten.

7. Kontinuierlicher Verbesserungsprozess

Durch eine kontinuierliche Überprüfung des ISMS, seiner Regelungen und deren Einhaltung wird das angestrebte Sicherheits- und Datenschutzniveau sichergestellt.

Abweichungen werden dahingehend analysiert, die Sicherheitssituation stetig zu verbessern und auf dem höchstmöglichen Niveau zu halten.

Im Rahmen eines kontinuierlichen Verbesserungsprozesses unterliegt die vorliegende Politik einer regelmäßigen Revision und Aktualisierung. Das bedeutet insbesondere:

- eine regelmäßige Überprüfung von Einhaltung, Aktualität und Wirksamkeit der Politik,
- eine mindestens jährliche Überprüfung (z. B. im Rahmen eines Audits).

8. Allgemeine Festlegungen

Herausgeber und verantwortlich für die Aktualisierung der Informationssicherheitspolitik ist der von der Geschäftsleitung bestellte ISB in Abstimmung mit dem ISMS-Koordinator der SWSZ Netz GmbH.

Die jeweils publizierte Fassung der Informationssicherheitspolitik ist die gültige und verbindliche Fassung. Sie ist in angemessenen Zeitabständen sowie bei signifikanten Änderungen zu revidieren.

Abweichende Regelungen sind mit dem ISB abzustimmen. Die grundlegenden Festlegungen der Richtlinie gelten uneingeschränkt und unmittelbar, unabhängig von der Erstellung eigener Regelungen.

Die Sicherheitsorganisation unterstützt alle Mitarbeiter und externe Dienstleister bei der Umsetzung der Sicherheitsrichtlinien und führt angemessene Kontrollen durch.