Informationssicherheitsleitlinie

Bearbeiter:	27.02.2023	Hr. Könitzer	ISB	
Prüfer:	27.02.2023	Hr. Könitzer	ISB	gez. Könitzer
Freigeber:	08.03.2022	Hr. Schäfer	GF SWSZ	gez. Schäfer
Freigeber:	08.03.2022	Hr. Belgardt	GF SWSZ Netz	gez. Belgardt

Änderungshistorie

Version	Autor	Datum	Beschreibung
0.1	secopan	30.05.2016	Neuerstellung
1.0	Erik Könitzer (EK)	22.08.2016	Layout-/Formulierungsanpassungen SWSZ
1.1	secopan BW	07.10.2016	Einarbeitung Behandlung von Sicherheitsvorfällen
2.0	EK	26.01.2018	Inhaltliche Überarbeitung nach Prüfung Soll-/ Istzustand
2.1	EK	17.05.2018	Anpassung Mail DSB
2.2	EK	03.01.2019	Revision & Ergänzung Pkt. 4
3.0	EK	31.01.2020	Revision
3.1	D. Lichtleitner	25.11.2020	Anpassungen Dokumentenlenkung
3.2	EK	02.02.2021	Revision, Anpassungen Informationsklassifizierung und Maßnahmen zum Schutz vor unbefugtem Zugriff auf Informationen (Clean Desk)
4.0	GF SWSZ/Netz	15.02.2021	Freigabe
4.1	EK	02.03.2022	Revision, inhaltliche Überarbeitung, Änderung der Klassifizierung
5.0	GF SWSZ/Netz	08.03.2022	Freigabe
5.0	EK	27.02.2023	Revision, Hinweis auf Dokument Rollen- und Verantwortlichkeiten

Inhalt

1. Ziel und Geltungsbereich....4
2. Rahmenbedingungen....4
2.1. Schutzziele....4
2.2. Gesetzliche Anforderungen....4
2.3. Adressaten....5
3. Informationsschutz....5
4. Sicherheitsmaßnahmen durch Richtlinien, Festlegungen und Prozesse....5
4.1. Sicherheitsmaßnahmen im täglichen Geschäftsbetrieb (Clean Desk)....6
5. Sicherheitsorganisation....7
6. Informationssicherheitsbewusstsein....7
7. Kontinuierlicher Verbesserungsprozess (KVP)....8
8. Maßregelungsprozess....8
9. Allgemeine Festlegungen....9

1. Ziel und Geltungsbereich

Die Stadtwerke Suhl/Zella-Mehlis GmbH (SWSZ) sowie die Stadtwerke Suhl/Zella-Mehlis Netz GmbH (SWSZ Netz) haben die Einführung eines Informationssicherheitsmanagementsystems (ISMS) mit der Erstzertifizierung im Jahr 2017 erfolgreich abgeschlossen.

Diese Leitlinie repräsentiert die Informationssicherheitspolitik der SWSZ und SWSZ Netz, deren Ziel es ist, Strategien, Maßnahmen und Prozesse zur Gewährleistung der Informationssicherheit zu definieren und die Schadensrisiken für die Unternehmen selbst, Kunden, Geschäftspartner und Behörden durch die Verhütung von Sicherheitsvorfällen und die Reduzierung ihrer potenziellen Auswirkungen zu minimieren.

2. Rahmenbedingungen

2.1. Schutzziele

Die Schutzziele hinsichtlich der Sicherstellung sämtlicher Geschäftsprozesse zur Lieferung von Strom, Gas und Fernwärme (SWSZ) sowie zur Gewährleistung des sicheren Stromnetz- und Gasnetzbetriebs (SWSZ Netz) 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.

2.2. Gesetzliche Anforderungen

Das ISMS der SWSZ und SWSZ Netz wird unter Einhaltung gesetzlicher Vorgaben und den Anforderungen der Normen DIN EN ISO/IEC 27001 und 27019, der Maßnahmen gemäß DIN EN ISO/IEC 27002 sowie des IT-Sicherheitskatalogs der BNetzA gemäß § 11 Abs. 1a EnWG betrieben.

Zur Gewährleistung des sicheren Netzbetriebs kommen weiterhin die Anforderungen der Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) und des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) zur Anwendung.

Die Wirksamkeit des ISMS ist gegenüber einer unabhängigen Zertifizierungsstelle nachzuweisen.

Zur Erfüllung der Meldepflicht von Sicherheitsvorfällen an das Bundesamt für Sicherheit in der Informationstechnik gemäß § 8b Abs. 4 BSI-Gesetz ist eine zentrale Kontakt- und Meldestelle eingerichtet.

2.3. Adressaten

Die Informationssicherheitsleitlinie gilt im Anwendungsbereich des ISMS als Handlungsanweisung für alle Mitarbeitenden sowie für Dritte, die

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

3. Informationsschutz

Schäden für das Unternehmen oder Dritte können entstehen, wenn Unbefugte bzw. Unberechtigte Kenntnis von internen Informationen erlangen oder auf informationsverarbeitende Systeme zugreifen und diese zum Nachteil der SWSZ und SWSZ Netz verwenden.

Daher müssen alle Berechtigten einen wirkungsvollen Schutz der Informationen sicherstellen, unabhängig von der Form, in der sie vorliegen.

Als berechtigt gelten interne Mitarbeitende der SWSZ und SWSZ Netz sowie Dritte gemäß Punkt 2.2, welche die Kenntnisnahme der Festlegungen der Informationssicherheitsleitlinie und der Informationssicherheitspolitik durch die Abgabe der

Verpflichtungserklärung Informationssicherheitsbewusstsein externe Dienstleister

verifiziert haben.

Mitarbeitende und berechtigte Dritte sind des weiteren zum Schutz des Eigentums verpflichtet. Zum Eigentum zählen alle Sach- und Vermögenswerte der SWSZ und SWSZ Netz.

4. Sicherheitsmaßnahmen durch Richtlinien, Festlegungen und Prozesse

Die Existenz, Sicherheit und Reputation der SWSZ und SWSZ Netz sind 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.

Mitarbeitende 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 Mitarbeitende oder externe Auftragnehmer ist verpflichtet, seien aktiven Beitrag zur Erkennung und Vermeidung von Sicherheitsvorfällen zu leisten
- informationsverarbeitende Systeme sind ausschließlich im Kontext der entsprechenden Richtlinien mit personalisierten Zugängen zu benutzen

4.1. Sicherheitsmaßnahmen im täglichen Geschäftsbetrieb (Clean Desk)

Durch den Informationseigner ist sicherzustellen, dass alle Informationen, welche nicht als öffentlich klassifiziert sind, sicher vor dem Zugriff unberechtigter Dritter, Beschädigung oder Verlust verwahrt werden, wenn der Arbeitsplatz für einen längeren Zeitraum verlassen wird.

Dabei ist es unerheblich, ob die Informationen auf Papier oder in digitalisierter Form vorliegen.

Dies betrifft neben dem PC-Bildschirm auch den Schreibtisch und im Raum vorhandene Ablage-möglichkeiten.

Folgende Empfehlungen sind im täglichen Geschäftsbetrieb anzuwenden:

- grundsätzliche Sperrung des PC-Bildschirms bei Abwesenheit (Win+L)
- Entfernen von sensiblen und vertraulichen Dokumenten vom Schreibtisch und Aufbewahrung an geeigneter Stelle
- Verschließen des Büros bei Abwesenheit

5. Sicherheitsorganisation

Gemäß Normforderungen sind in der Sicherheitsorganisation die nachfolgenden Rollen und Verantwortlichkeiten festgelegt:

- Geschäftsführungen der SWSZ und SWSZ Netz
  - Gesamtverantwortung für den Betrieb und die kontinuierliche Weiterentwicklung des ISMS
  - Festlegen der Ziele des ISMS und der Informationssicherheitspolitik
  - Bereitstellung der notwendigen Ressourcen
  - Bestellung des ISB
  - Etablierung des ISMS in der Unternehmenskultur („Leben des ISMS“)
- Informationssicherheitsbeauftragter (ISB)
  - Führung des ISMS-Teams und Sicherstellung der Wirksamkeit des ISMS
  - Umsetzung der Informationssicherheitspolitik, der festgelegten Ziele und des kontinuierlichen Verbesserungsprozesses
  - Integration des ISMS in die Geschäftsprozesse
  - Eskalation etwaiger Risiken an die Geschäftsleitung
  - Beratung und Schulung der Mitarbeitenden zu Themen der Informationssicherheit
  - Erfüllung von Nachweis- und Berichtspflichten
  - Auditmanagement
- Abteilungsleiter IT/Administration/Digitales
- IT-Koordinator und ISMS-Koordinator SWSZ Netz
- Datenschutzbeauftragter
- ISMS-Team (auf Anforderung GF oder ISB)
  - Das ISMS-Team wird durch den Systemadministrator, Fach- und Führungskräfte der Fachabteilungen sowie die Stabsstelle Allgemeine Verwaltung/Personal auf Anforderung der Geschäftsführungen oder des ISB ergänzt.

Die Informationssicherheitsrollen und -verantwortlichkeiten sind im Dokument AN_5.3_Aufgabenbeschreibungen und Kommunikation_Vx-y definiert.

6. Informationssicherheitsbewusstsein

Gemäß den Anforderungen der Norm, dass sich Personen, die entsprechende Tätigkeiten ausüben, Folgendem bewusst sind, wurde in der SWSZ und SWSZ Netz festgelegt, dass:

- die Mitarbeiterinnen und Mitarbeiter die Informationssicherheitspolitik und die Informationssicherheitsleitlinie der Unternehmen kennen und anwenden,

- neue Mitarbeiterinnen und Mitarbeiter durch den ISB bei ihrem Eintritt in die Informationssicherheitspolitik, die Informationssicherheitsleitlinie sowie grundlegende Richtlinien eingewiesen werden,
- alle Mitarbeiterinnen und Mitarbeiter in regelmäßigen Zeitabständen durch den ISB geschult werden (z.B. per E-Mail, über das Intranet bzw. Schulungsplattformen, über themenspezifische Workshops und Sensibilisierungskampagnen),
- sich die Mitarbeiterinnen und Mitarbeiter ihres Beitrags, den sie zur Wirksamkeit des ISMS leisten bewusst sind und die Vorteile verbesserter Informationssicherheitsleistung kennen,
- von externen Auftragnehmern die „Verpflichtungserklärung zum Informationssicherheitsbewusstsein externer Auftragnehmer“ vor Beginn ihrer Tätigkeit abzufordern ist.

7. Kontinuierlicher Verbesserungsprozess (KVP)

Die Wirksamkeit und Weiterentwicklung des ISMS wird jährlich, sowohl in internen Audits, als auch durch eine unabhängige Zertifizierungsstelle überprüft.

Prüfungsgegenstände sind insbesondere

- Zugriffsmöglichkeiten auf Informationen,
- Zugangsmöglichkeiten zu informationsverarbeitenden System und sensiblen Bereichen,
- Kontrollen im Zusammenhang mit Informationen, Verwaltung von Informationen, einschließlich der Trennung von Rollen und unabhängige Genehmigung bzw. Überprüfung von Transaktionen,
- Maßnahmen zur Behebung von Störungen,
- Einhaltung der Konformität zu Normen und Vorgaben.

Abweichungen, Hinweise und Verbesserungspotentiale aus den Auditierungen werden analysiert und fließen durch die Anwendung geeigneter Maßnahmen zur qualitativen Verbesserung sowie zur Erreichung der festgelegten Informationssicherheitsziele in den Betrieb des ISMS ein.

8. Maßregelungsprozess

Als Verstöße gelten beabsichtigte oder grob fahrlässige Handlungen, welche

- eine Kompromittierung der Reputation der SWSZ und SWSZ Netz darstellen,
- eine Bedrohung für die Sicherheit der Mitarbeitenden sowie des Vermögens der SWSZ und SWSZ Netz darstellen,
- die Sicherheit von Informationen oder informationsverarbeitenden Systemen hinsichtlich deren Verfügbarkeit, Integrität und Vertraulichkeit gefährden,
- durch Kompromittierung der Sicherheit von Informationen oder informationsverarbeitenden Systemen der SWSZ und SWSZ Netz tatsächlichen oder potenziellen finanziellen Verlust zufügen,

- den unberechtigten Zugriff auf Informationen oder informationsverarbeitende Systeme, deren Preisgabe und/oder Änderung beinhalten,
- die Nutzung von Unternehmensinformationen für illegale Zwecke beinhalten.

Die Nichteinhaltung oder bewusste Verletzung der Informationssicherheitsleitlinie kann zu einer der folgenden Maßnahmen führen:

- disziplinarische oder arbeitsrechtliche sowie straf- und/oder zivilrechtliche Konsequenzen,
- Haftung und Regressforderungen.

9. Allgemeine Festlegungen

Herausgeber und verantwortlich für die Aktualisierung der Informationssicherheitsleitlinie ist der von den Geschäftsführungen bestellte ISB in Abstimmung mit dem ISMS-Koordinator SWSZ Netz und der IT-Abteilung der SWSZ.

Die jeweils publizierte Fassung der Informationssicherheitsleitlinie 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 Mitarbeitenden und externe Auftragnehmer bei der Umsetzung der Sicherheitsrichtlinien und führt angemessene Kontrollen durch.