Informationssicherheitspolitik

Rahmenbedingungen, Strategien und Ziele

Stadtwerke Suhl/Zella-Mehlis 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 SWSZ	11.02.2025	Freigabe
7.0	EK	26.03.2026	Komplette Neufassung mit Ergänzung NIS2-spezifischer Anforderungen
7.0	Stefan Franke (SF)	08.04.2026	Dokumentenprüfung NIS2-Koordinator
7.0	GF SWSZ	10.04.2026	Freigabe

Inhalt

1. Ziel und Geltungsbereich

Die Informationssicherheitspolitik legt die verbindlichen Leitlinien der SWSZ GmbH für den Schutz von Informationen, informationsverarbeitenden Systemen, digitalen Diensten, unterstützenden Prozessen sowie relevanten betriebstechnischen Umgebungen fest.

Sie schafft den gemeinsamen Handlungsrahmen für Prävention, Erkennung, Bewältigung und Nachbereitung von Sicherheitsereignissen. Diese Politik konkretisiert damit zugleich die Anforderungen der ISO/IEC 27001 an Kontext, Führung und Zielausrichtung des ISMS sowie die NIS2-Anforderungen an Leitungsverantwortung und risikobasierte Cybersicherheitsmaßnahmen.

Ziel ist es, die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von Informationen sowie die Belastbarkeit der für die Leistungserbringung erforderlichen Systeme zu gewährleisten. Die Politik dient zugleich dem Schutz der Versorgung, der Geschäftsprozesse, der gesetzlichen und vertraglichen Verpflichtungen, der Kundeninteressen sowie der Reputation der SWSZ GmbH.

Die Festlegungen gelten für alle Mitarbeiterinnen und Mitarbeiter, Führungskräfte sowie für externe Parteien, soweit diese im Auftrag der SWSZ GmbH Informationen verarbeiten, Systeme nutzen oder Zugang zu relevanten Standorten, Netzen oder Daten erhalten.

2. Stellenwert und Grundsätze der Informationssicherheit

Informationssicherheit ist ein wesentlicher Erfolgsfaktor für die sichere und verlässliche Aufgabenerfüllung der SWSZ GmbH. Sie ist integraler Bestandteil von Unternehmenssteuerung, Prozessgestaltung, Projektarbeit, Beschaffung, Betrieb, Dienstleistersteuerung und Veränderungsvorhaben.

Die SWSZ GmbH verfolgt einen risikobasierten, angemessenen und wirksamen Sicherheitsansatz. Sicherheitsmaßnahmen werden nicht isoliert betrachtet, sondern in Abhängigkeit von Schutzbedarf, Bedrohungslage, Kritikalität der Prozesse, Abhängigkeiten sowie den möglichen Auswirkungen auf Versorgung, Rechtssicherheit, Vermögenswerte und Vertrauen interessierter Parteien festgelegt.

3. Leitungsverantwortung und Sicherheitsorganisation

Die Geschäftsleitung trägt die Gesamtverantwortung für Informationssicherheit, bestätigt diese Politik, stellt Ressourcen bereit, legt Sicherheitsziele fest, bewertet wesentliche Risiken und überwacht die Wirksamkeit des ISMS.

Das ISMS-Team koordiniert, berät die Geschäftsleitung, initiiert Verbesserungen, begleitet Risiken, Vorfälle, Schulungen, Audits und Richtlinienpflege und berichtet regelmäßig sowie anlassbezogen an die Leitung. Fachbereiche, IT, Prozesssteuerung, Datenschutz, Personal und weitere relevante Stellen wirken im jeweiligen Verantwortungsbereich verbindlich mit.

Führungskräfte sind dafür verantwortlich, die Anforderungen dieser Politik in ihren Bereichen umzusetzen, Abweichungen zu adressieren, Mitarbeiterinnen und Mitarbeiter zu sensibilisieren und Sicherheitsaspekte frühzeitig in Projekte, Beschaffungen und betriebliche Änderungen einzubringen.

4. Risikomanagement und Schutzbedarf

Die SWSZ GmbH identifiziert, bewertet und behandelt Informationssicherheitsrisiken fortlaufend und anlassbezogen. Hierzu gehören insbesondere Risiken aus Cyberangriffen, Fehlbedienung, technischen Ausfällen, Schwachstellen, Abhängigkeiten von Dritten, Änderungen im Betrieb, physischen Ereignissen und regulatorischen Anforderungen.

Informationswerte, Systeme, Dienstleistungen und Geschäftsprozesse sind nach Schutzbedarf und Kritikalität zu bewerten. Die Risikobehandlung umfasst geeignete organisatorische, personelle, technische und physische Maßnahmen, deren Umsetzungsstand, Wirksamkeit und Restrisiken dokumentiert werden.

Bei wesentlichen Änderungen, neuen Projekten, neuen Dienstleistern, Cloud-Nutzung, Fernwartung, relevanten Änderungen in der Prozesssteuerung, erheblichen Vorfällen oder neuen Bedrohungen ist eine erneute Risikobetrachtung verpflichtend durchzuführen.

5. Operative Sicherheitsgrundsätze

Alle für den ISMS-Anwendungsbereich relevanten Informationen und Systeme sind inventarisiert, Verantwortlichkeiten sind festgelegt und Zugriffe werden eindeutig zugeordnet. Personalisierte Konten, starke Authentisierung, kontrollierte Rechtevergabe, Protokollierung sicherheitsrelevanter Aktivitäten und sichere Administrationsverfahren sind verbindliche Mindestanforderungen.

Systeme und Anwendungen sind gehärtet zu betreiben, auf einen genehmigten Soll-Zustand auszurichten und über definierte Verfahren für Patch-, Schwachstellen-, Änderungs- und Konfigurationsmanagement zu steuern. Backup-, Wiederherstellungs-, Protokollierungs- und Überwachungsanforderungen sind nach Kritikalität festzulegen.

6. Sicherheitsvorfälle und Meldepflichten

Sicherheitsereignisse, Schwachstellen, Auffälligkeiten und bestätigte Vorfälle sind unverzüglich über die festgelegten Meldewege an die zuständigen internen Stellen zu melden. Die SWSZ GmbH betreibt hierzu verbindliche Prozesse für Erkennung, Erstbewertung, Klassifizierung, Eskalation, Eindämmung, Beweissicherung, Wiederherstellung und Nachbereitung.

Potenziell erhebliche Cybervorfälle sind so zu behandeln, dass externe regulatorische Meldepflichten fristgerecht erfüllt werden können. Entscheidungen, Zeitpunkte, betroffene Systeme, Auswirkungen, Gegenmaßnahmen und Lessons Learned sind revisionssicher zu dokumentieren.

Datenschutzverletzungen, strafrechtlich relevante Sachverhalte, versorgungsrelevante Auswirkungen sowie Vorfälle mit Lieferketten- oder Dienstleisterbezug sind mit den jeweils zuständigen Stellen koordiniert zu behandeln.

7. Betriebskontinuität und Wiederherstellung

Die SWSZ GmbH stellt durch angemessene Notfallvorsorge, Wiederanlaufplanung und Wiederherstellungsverfahren sicher, dass kritische Geschäftsprozesse und unterstützende Systeme auch bei Störungen, Cybervorfällen oder Ausfällen in angemessener Zeit fortgeführt oder wiederhergestellt werden können.

Notfall- und Wiederherstellungspläne, Kommunikationswege, Ersatzverfahren, Verantwortlichkeiten, Wiederanlaufprioritäten und Abhängigkeiten von internen oder externen Leistungen sind dokumentiert und regelmäßig getestet.

Wiederherstellungen dürfen nur kontrolliert, nachvollziehbar und nach Freigabe in den Produktivbetrieb überführt werden. Dabei ist sicherzustellen, dass Kompromittierungen nicht übernommen und Ursachen sowie Lerneffekte berücksichtigt werden.

8. Beschäftigte, Sensibilisierung und Sicherheitskultur

Alle Beschäftigten und relevanten externen Parteien müssen die für ihre Rolle geltenden Sicherheitsanforderungen kennen, verstehen und anwenden. Sicherheitsrelevante Pflichten sind Bestandteil von Onboarding, laufender Sensibilisierung, fachbezogener Qualifizierung und Führungskräfteverantwortung.

Personen mit erhöhten Rechten, Sicherheitsfunktionen oder besonderer Verantwortung für IT-, OT-, Projekt-, Beschaffungs-, Notfall- oder Lieferkettenprozesse erhalten eine vertiefte, rollenbezogene Schulung. Die Wirksamkeit von Schulungen und Awareness-Maßnahmen ist zu bewerten und bei Bedarf anzupassen.

Die SWSZ GmbH fördert eine Sicherheitskultur, in welcher Meldungen zu Schwachstellen, Fehlern und Verbesserungsmöglichkeiten ohne sachfremde Hemmnisse erfolgen können. Vorsätzliche oder grob fahrlässige Verstöße bleiben hiervon unberührt.

9. Dienstleister, Lieferkette und externe Parteien

Externe Dienstleister, Lieferanten, Cloud-Anbieter, Wartungsunternehmen, Projektpartner und sonstige Dritte dürfen nur eingebunden werden, wenn Informationssicherheitsanforderungen risikoorientiert bestimmt, vertraglich verankert und während des gesamten Lebenszyklus überwacht werden.

Vor Beauftragung sowie bei wesentlichen Änderungen sind Sicherheitsanforderungen, Zugriffsmodelle, Unterstützungsleistungen im Störungs- und Ereignisfall, Protokollierungs- und Nachweispflichten, Schutz von Daten, Unterauftragnehmer, Exit-Regelungen und Wiederherstellungsaspekte zu berücksichtigen.

Abhängigkeiten in der Lieferkette sind im Rahmen des ISMS transparent zu machen. Kritische externe Leistungen unterliegen einer verstärkten Steuerung, regelmäßigen Überprüfung und dokumentierten Risikobewertung.

10. Dokumentation, Nachweise und Wirksamkeitskontrolle

Die SWSZ GmbH dokumentiert die wesentlichen Elemente ihres ISMS, einschließlich Politik, Zielen, Rollen, Risiken, Maßnahmen, Vorfällen, Schulungen, Prüfungen, Managemententscheidungen und Verbesserungen.

Die Wirksamkeit der Informationssicherheitsmaßnahmen wird durch Kennzahlen, Reviews, Audits, Tests, Übungen, Schwachstellenbewertungen, Vorfallauswertungen und Managementbewertungen überwacht. Festgestellte Abweichungen und Verbesserungspotenziale führen zu dokumentierten Korrektur- und Verbesserungsmaßnahmen.

Die Geschäftsleitung erhält regelmäßig ein adressatengerechtes Bild über Sicherheitslage, Risiken, Vorfälle, Reifegrad, Status wesentlicher Maßnahmen und des aktuellen Handlungsbedarfs.

11. Kommunikation und Veröffentlichung

Diese Politik wird innerhalb der SWSZ GmbH angemessen bekannt gemacht und den betroffenen internen sowie externen Parteien zugänglich gemacht, soweit dies für ihre Aufgaben, Pflichten oder vertraglichen Beziehungen erforderlich ist.

Sofern erforderlich, ist bei Schriftverkehr mit externen Dienstleistern, Geschäftspartnern oder Institutionen auf die im Internet unter swsz.de → DIE SWSZ → Informationssicherheit veröffentlichte Informationssicherheitspolitik hinzuweisen.

Für sicherheitsrelevante Kommunikation gelten definierte Zuständigkeiten, Freigaben und Kommunikationswege. Externe Kommunikation zu Sicherheitsvorfällen, regulatorischen Sachverhalten oder sicherheitsrelevanten Krisen erfolgt ausschließlich durch autorisierte Stellen in abgestimmter Form.

Untergeordnete Richtlinien, Verfahren und Handlungsanweisungen konkretisieren diese Politik. Sie müssen konsistent, aktuell und für den jeweils betroffenen Personenkreis verfügbar sein.

12. Referenzierung und normative Zuordnung

Abschnitt	ISO/IEC 27001	NIS2-Richtlinie
1	Kapitel 4, 5 und 6	Art. 20 und Art. 21 zur Leitungsverantwortung und zu risikobasierten Sicherheitsmaßnahmen
2	Kapitel 4 bis 8, risikobasiertes ISMS-Modell	Art. 21 Abs. 1 und 2 zu geeigneten, verhältnismäßigen und wirksamen technischen, operativen und organisatorischen Maßnahmen
3	Kapitel 5 (Führung), Kapitel 7 (Unterstützung) und Kapitel 9 (Bewertung der Leistung)	Art. 20 zur Billigung, Überwachung und Verantwortung der Leitungsorgane sowie Art. 21 zu Governance-nahen Risikomanagementmaßnahmen
4	Kapitel 6 und 8 sowie Anhang A thematisch A.5 bis A.8	Art. 21 Abs. 2, insbesondere Risikoanalyse, Sicherheit bei Beschaffung, Entwicklung,

		Wartung, Schwachstellenbehandlung und Lieferkettensicherheit
5	Kapitel 8 und Anhang A, insbesondere organisatorische, personelle, physische und technologische Maßnahmen	Art. 21 Abs. 2, insbesondere Ereignisbehandlung, Betriebskontinuität, Backup, Sicherheit bei Erwerb/Entwicklung/Wartung, Schwachstellenmanagement, Kryptografie, sichere Authentisierung und gesicherte Kommunikation
6	Kapitel 8 (operativer Betrieb) und Kapitel 10 (Verbesserung), Anhang A thematisch zum Incident Management	Art. 21 Abs. 2 Buchst. b sowie Art. 23 zu gestuften Meldepflichten und fortlaufender Berichterstattung bei erheblichen Vorfällen
7	Kapitel 8 und 9 sowie Anhang A thematisch zu IT-Verfügbarkeit und Backups	Art. 21 Abs. 2 insbesondere zu Betriebskontinuität, Krisenmanagement und Backup-/Wiederherstellungsmanagement
8	Kapitel 5 und Kapitel 7 (Kompetenz, Bewusstsein und Kommunikation)	Art. 20 zur Leitungsverantwortung sowie Art. 21 Abs. 2 zu Cyberhygiene, Schulungen und sicherheitsbewusstem Verhalten
9	Kapitel 4.2, Kapitel 8 und Anhang A thematisch zu Lieferantenbeziehungen	Art. 21 Abs. 2 Buchst. d zur Sicherheit der Lieferkette und zu sicherheitsbezogenen Beziehungen zwischen Einrichtungen und ihren unmittelbaren Anbietern oder Dienstleistern
10	Kapitel 7.5, 9 und 10	Art. 21 zur dokumentierbaren Umsetzung geeigneter Maßnahmen sowie Art. 20 zur Überwachung durch die Leitungsorgane
11	Kapitel 5 und Kapitel 7 (Kommunikation, dokumentierte Information)	Art. 21 und Art. 23, soweit Kommunikations- und Meldeprozesse für erhebliche Vorfälle betroffen sind

13. Schlussbestimmungen

Diese Informationssicherheitspolitik ist von der Geschäftsleitung zu genehmigen, bekannt zu machen und in regelmäßigen Abständen sowie anlassbezogen zu überprüfen.

Bei signifikanten Änderungen von Geschäftsmodell, Bedrohungslage, eingesetzten Technologien, gesetzlichen Anforderungen oder dem ISMS-Anwendungsbereich ist die Politik zu revidieren.

Die Schlussbestimmungen stellen sicher, dass die Informationssicherheitspolitik sowohl als oberste Leitlinie des ISMS im Sinne der ISO/IEC 27001 als auch als Governance-wirksames Steuerungsdokument im Sinne der NIS2-Richtlinie fortlaufend gepflegt, überprüft und weiterentwickelt wird.

Die konkretisierenden Anforderungen werden in untergeordneten Richtlinien, Verfahren, Standards, Notfall- und Betriebshandbüchern sowie in technischen und organisatorischen Maßnahmen umgesetzt.

Suhl, 10.04.2026

Tino Schäfer - Geschäftsführer