Informationssicherheitsleitlinie

Richtlinie zur Einhaltung der Informationssicherheit
der Stadtwerke Wiesbaden Netz GmbH

Status: Freigabe

Version: 3.2

Autor: Nils Amthor

Freigegeben durch: Peter Lautz

Datum: 18.10.2023

Verantwortliche Personen / Änderungsdienst:

Peter Lautz	Geschäftsführung
Roberto Kumpf	Informationssicherheitsbeauftragter (ISB)
Nils Amthor	stellv. Informationssicherheitsbeauftragter (ISB)
Arno Kügler	Mitarbeiter im ISMS-Team
Marcel Nikol	Mitarbeiter im ISMS-Team
Simon Reichel	Mitarbeiter im ISMS-Team

Überprüft am: 11.10.2023

Überprüft durch: ISMS-Team

Klassifizierung: öffentlich

Verteilerkreis: Alle Mitarbeiter SW Netz, sowie externe Dienstleister

Zertifizierungsturnus
2023-2025

Dokumentenhistorie

Version	Datum	Bearbeitet durch	Änderung
0.1	13.01.2017	Klaus Maurer	
0.2	01.02.2017	Kumpf, Roberto	Redaktionelle Änderungen
1.0	04.05.2017	Maurer, Klaus	Redaktionelle Änderungen/Formatanpassungen
1.1	05.06.2018	Kumpf, Roberto	Anpassung Kap. 3.5 (Link zu wesentlichen Dokumenten im Intranet)
1.2	05.04.2019	Schott, Armin	Anpassungen ISO/IEC auf akt. Versionen
2.0		Lautz, Peter	Freigabe
2.1	23.09.2021	Schott, Armin	Anpassung fehlerhafte Verlinkung
2.2	23.09.2021	Schott, Armin	Löschen Rollen u. Verantwortliche, da im ISMS-Handbuch dokumentiert.
3.0	08.10.2021	Schott, Armin	Korrektur Dokumentenbezeichnung
3.1	14.09.2022	ISMS-Team	Kapitel 1 verkürzt; Kapitel 3.4 angepasst; Kapitel 3.5 Grafik und Links entfernt
3.2	22.09.2023	Nils Amthor	Überführung in neue Dokumentenstruktur

Inhaltsverzeichnis

1. Einleitung

Die Geschäftsführung und alle Mitarbeiter der *Stadtwerke Wiesbaden Netz GmbH* sind verpflichtet die Informationssicherheitsleitlinie einzuhalten. Dies gilt auch für externe Dienstleister, denen Zugang zu informationsverarbeitenden Systemen oder Informationen der *Stadtwerke Wiesbaden Netz GmbH* gewährt wird.

Verstöße gegen diese Informationssicherheitsleitlinie können zu Disziplinarmaßnahmen, bis hin zu arbeits-, straf- und/oder zivilrechtlichen Verfolgung führen.

2. Geltungsbereich

Die vorliegende Informationssicherheitsleitlinie gilt für alle Mitarbeiter und externe Dienstleister der *Stadtwerke Wiesbaden Netz GmbH.* Die Geschäftsführung und alle Mitarbeiter der *Stadtwerke Wiesbaden Netz GmbH* sind verpflichtet die Informationssicherheitsleitlinie einzuhalten

3. Informationssicherheit

Im nachfolgenden werden die jeweiligen Grundlagen zur Informationssicherheit definiert.

3.1 Stellenwert der Informationssicherheit

Informationen sind grundlegende Faktoren für den Geschäftsbetrieb und für die Erreichung der Unternehmensziele und stellen Unternehmenswerte der *Stadtwerke Wiesbaden Netz GmbH* dar.

Alle wesentlichen, strategischen und operativen Funktionen und Aufgaben werden durch informationsverarbeitende Systeme maßgeblich unterstützt.

Alle Beteiligten *(Kunden, Dienstleister, Lieferanten, Partner, Gesellschafter, etc.)* müssen sich darauf verlassen können, dass die *Stadtwerke Wiesbaden Netz GmbH* die Sicherheitsverantwortung für die von ihr verarbeiteten Informationen gewissenhaft wahrnimmt und vor missbräuchlicher Verwendung schützt.

3.2 Schutzziele der Informationssicherheit

Ziel des Managements der Informationssicherheit ist es, im Rahmen der gesetzlichen Anforderungen, eine kontinuierliche und wirtschaftlich angemessene Steuerung solcher Risiken sicher zu stellen, die in Verbindung mit der Verarbeitung, dem Transport und der Speicherung von Informationen stehen. Dies gilt insbesondere für Informationen, die für die Sicherheit des Netzbetriebes erforderlich sind.

Die Informationssicherheit betrifft Informationen, die in elektronischer oder gedruckter / schriftlicher Form vorliegen aber auch mündlich übermittelte Informationen, z. B. in Telefonaten oder Gesprächen an öffentlichen Orten.

Zur Wahrung der Informationssicherheit dienen die folgenden Schutzziele:

- **Vertraulichkeit**
  Vertraulichkeit bedeutet Schutz vor Offenlegung von Informationen ohne Erlaubnis des Eigentümers.

- **Integrität**
  Integrität bedeutet Schutz vor Modifikation von Informationen durch nicht berechtigte Personen und stellt die Richtigkeit, Konsistenz und Vollständigkeit von Informationen dar.
- **Verfügbarkeit**
  Verfügbarkeit bedeutet, dass Prozesse, Informationen, Funktionen und Informationssysteme immer dann verfügbar sind, wenn ein autorisierter Benutzer sie bearbeiten bzw. in Anspruch nehmen will. „Verfügbar" heißt in diesem Zusammenhang auch, dass der Zugriff auf Informationen, Funktionen und Betriebsmittel bedarfsgerecht gewährleistet ist.

3.3 Informationssicherheitsgrundsätze

Das Fundament dieser Informationssicherheitsleitlinie bilden die folgenden Grundsätze, an denen sich sämtliche Sicherheitsmaßnahmen und –vorgaben ausrichten und die für alle Mitarbeiter der *Stadtwerke Wiesbaden Netz GmbH* verbindlich sind.

1. Für Unternehmenswerte wie Informationen, IT-Systeme und IT-Anwendungen sind Eigentümer benannt, die für die Sicherheit der jeweiligen Unternehmenswerte verantwortlich sind.
2. Risiken aus der Nutzung der Informationen und Informationssysteme sind frühzeitig zu identifizieren und auf ein akzeptiertes Restrisiko zu minimieren.
3. Kosten und Nutzen von Sicherheitsmaßnahmen stehen in einem angemessenen wirtschaftlichen Verhältnis.
4. Vorgaben und Maßnahmen orientieren sich an anerkannten Standards und Best Practices zur Informationssicherheit.
5. Gesetzliche, regulatorische, vertragliche und sonstige Vorgaben für die Informationssicherheit sind zu identifizieren und durch angemessene Maßnahmen umzusetzen.
6. Zugriff, Zugang und Zutritt zu den Informationswerten sind auf das notwendige Maß zu beschränken.
7. Alle wesentlichen Aktivitäten und Ereignisse im Bereich Informationssicherheit müssen transparent und im erforderlichen Umfang nachvollziehbar sein. Verfahren für den Betrieb bzw. die Wiederherstellung des Betriebs der wesentlichen Informationssysteme sind zu dokumentieren. Sofern erforderlich, ist ein Notfallplan und ein Wiederanlaufplan zu erstellen und in das Notfallmanagement der *Stadtwerke Wiesbaden Netz GmbH* zu integrieren.
8. Für die an der Verarbeitung von Informationen beteiligten Mitarbeiter müssen angemessene Vorkehrungen zur Gewährleistung der Vertrauenswürdigkeit getroffen werden.
9. Die Mitarbeiter werden hinsichtlich des sicheren Umgangs mit Informationswerten informiert, geschult und sensibilisiert. Sie sind verpflichtet, die entsprechenden Vorgaben umzusetzen.
10. Die Wirksamkeit der Vorgaben und Maßnahmen zur Informationssicherheit werden kontinuierlich überprüft und verbessert.

3.4 Ziele des Informationssicherheitsmanagementsystems

Abgeleitet von den Zielen der Informationssicherheit und den Informationssicherheitsgrundsätzen, werden folgende Ziele für das Informationssicherheitsmanagementsystem der Stadtwerke Wiesbaden Netz GmbH definiert.

1. Die Unterstützung des Unternehmens bei der Erreichung der Unternehmensziele und Sicherung der Unternehmenswerte.
2. Die Unterstützung beim täglichen ausfallfreien Betrieb des Leitsystems rund um die Uhr.
3. Ein Risikomanagement zur Reduktion von Risiken auf ein angemessenes Risikoniveau.
4. Gewährleistung einer kontinuierlichen Information und Schulung der Mitarbeiter zur Umsetzung der Informationssicherheitsvorgaben.
5. Gewährleistung einer kontinuierlichen Überprüfung der Vorgaben und Maßnahmen zur Informationssicherheit.
6. Die Schaffung von Resilienz in Krisenfällen.
7. Die Überführung von gesetzlichen Vorgaben der Informationssicherheit in anerkannte Best Practices.

3.5 Methodik für die Informationssicherheit

Das ISMS der *Stadtwerke Wiesbaden Netz GmbH* wird anhand von Leitlinien, Richtlinien und Sicherheitskonzepten geführt. Diese sind innerhalb der relevanten Geschäftsprozesse umzusetzen.

Die in Kapitel 3.3 definierten Informationssicherheitsgrundsätze werden in folgenden Richtlinien und Sicherheitskonzepten konkretisiert:

Dokumente der Ebene 2 sind im ISMS-Managementhandbuch und im ISMS-Handbuch zusammengefasst.

- Scope Dokumentation

Das ISMS gilt grundsätzlich in allen für die Netzsteuerung wesentlichen Prozessen und wird zunächst in Teilen des Unternehmens eingeführt. Die Eingrenzung des Scopes erfolgt im Dokument ISMS-Handbuch.

- ISMS-Managementhandbuch

Das ISMS-Managementhandbuch beschreibt die innere Struktur des ISMS. Es macht Vorgaben zur Struktur des ISMS und der Sicherheitsorganisation.

- Informationssicherheitsrisikomanagement

Die Richtlinie zum Informationssicherheitsrisikomanagement (ISRM) legt die Methodik zur Durchführung des Risikomanagements fest. Sie regelt die Identifizierung, Bewertung und Behandlung von Risiken für Informationswerte des Unternehmens.

- Bewertung der Leistung des ISMS

In der Richtlinie zur Bewertung der Leistung des ISMS werden Prozesse und Methoden zur Messung der Wirksamkeit des ISMS festgelegt.

- Lenkung von dokumentierten Informationen

Die Richtlinie zum Dokumentenlenkung enthält Vorgaben zum Umgang mit Dokumenten, insbesondere zur Klassifizierung von Informationen und zur Dokumentenlenkung.

Dokumente der Ebene 3 sind in den Informationssicherheitsmaßnahmen zusammengefasst.

- Benutzerrichtlinie

Die Benutzerrichtlinie enthält Vorgaben zum Umgang mit Informationswerten und IT-Systemen die durch alle Mitarbeiter umgesetzt werden müssen.

- Personelle Sicherheit

Das Sicherheitskonzept zur personellen Sicherheit enthält Vorgaben für die Informationssicherheitsaspekte in den Personalprozessen für die Mitarbeiter der *Stadtwerke Wiesbaden Netz GmbH*. Dies umfasst sämtliche Personalprozesse vor, während und nach der Beschäftigung bei der *Stadtwerke Wiesbaden Netz GmbH*.

- Physische Sicherheit

Das Sicherheitskonzept zur physischen Sicherheit beschreibt Maßnahmen, deren Umsetzung und Aufrechterhaltung der physischen Sicherheit dienen. Hierzu zählen beispielsweise Zutritts Kontrollsysteme, Stromversorgung und Klimatisierung von Technikräumen bzw. Rechenzentren.

- Security Incident Management (Umgang mit Sicherheitsvorfällen)

Das Sicherheitskonzept zum Umgang mit Sicherheitsvorfällen beschreibt Prozesse zur Meldung, Dokumentation und Behandlung von Sicherheitsvorfällen.

- Notfallmanagement (Business Continuity Management – BCM)

Im Sicherheitskonzept zum BCM werden Anforderungen an die Informationssicherheit für das Notfallmanagement definiert. Hierin sind Prozesse und Maßnahmen beschrieben, die im Not- oder Katastrophenfall das erforderliche Niveau an Informationssicherheit bei der Aufrechterhaltung des Geschäftsbetriebs sicherstellt.

- Compliancekonzept (interne und externe Vorgaben)

Das Compliancekonzept beschreibt, welche internen und externen Vorgaben für die *Stadtwerke Wiesbaden Netz GmbH* gelten und zu befolgen sind sowie die hierfür erforderlichen Prozesse.

Statement of Applicability (SoA / Erklärung zur Anwendbarkeit)

Nicht alle Maßnahmen der ISO/IEC 27001: sowie der ISO/IEC TR 27019: (jeweils in aktueller Version) müssen in jedem Unternehmen umgesetzt werden. In der Erklärung zur Anwendbarkeit werden anwendbare und nicht anwendbare Maßnahmen bei der *Stadtwerke Wiesbaden Netz GmbH* jeweils mit Begründung dokumentiert.

Betriebshandbuch

In den Betriebshandbüchern werden für IT- und TK-Systeme die Verfahren für den Betrieb und die Wiederherstellung des Betriebes für Dritte nachvollziehbar dokumentiert.

3.6. Dokumente

3.6.1. Intern

Die Dokumente sind im Intranet einsehbar:

„Unternehmenshandbuch“ -> „Stadtwerke Wiesbaden Netz GmbH“ -> „ISMS“,

3.6.2. Extern

Für Externe unter folgendem Link:

ISMS – Stadtwerke Wiesbaden Netz GmbH (sw-netz.de)

4. Kontinuierliche Prüfung und Verbesserung

Zur kontinuierlichen Bewertung und Verbesserung des ISMS und seiner Prozesse ist die Einführung eines Auditprogramms zur Informationssicherheit erforderlich. Dieses bietet die Möglichkeit, Abweichungen von den Zielen des ISMS zu identifizieren und zeitnah zu bewerten. Die Prüfungen werden jährlich durchgeführt.

5. Unterzeichnung

Durch die Unterzeichnung des Geschäftsführers der *Stadtwerke Wiesbaden Netz GmbH* ist diese ab sofort gültig und in allen enthaltenden Punkten ausnahmslos anzuwenden. Änderungen bzw. abweichende Handhabungen dieser Richtlinie sind nur mit Zustimmung des Geschäftsführers erlaubt. Dies muss schriftlich dokumentiert werden.

Wiesbaden, den 18.10.23

Peter Lautz, Geschäftsführer