ovag Netz
Planung. Bau. Betrieb.

Informationssicherheits-Leitlinie

gültig ab 01.11.2019
Version: 1.1
Stand: freigegeben
Klassifikation: öffentlich
ovag Netz GmbH

Änderungshistorie:

Version	Datum	Autor	Änderungshinweise
0.1	11.10.2018	Carsten Zeiger	Erster Entwurf
1.0	17.10.2018	Axel Finkeldey	Freigabefassung
1.1	02.10.2019	Finkeldey	Logo angepasst, oE entfernt

Qualitätssicherung:

Version	Datum	Prüfer	Änderungshinweise
1.0	17.10.2018	Axel Finkeldey	
1.1	09.10.2019	Kreuz	

Freigabeprotokoll:

Version	Datum	Genehmigt durch	Titel/Rolle
1.0	08.11.2018	Peter-Hans Hög	Geschäftsführer
1.1	23.10.2019	Peter-Hans Hög	Geschäftsführer

Klassifikation:

Version	Datum	Klassifiziert durch	Klassifikation
0.1	13.06.2016	Carsten Zeiger	öffentlich
1.0	17.10.2018	Axel Finkeldey	öffentlich
1.1	02.10.2019	Finkeldey	öffentlich

Dokumentenverteilung:

Veröffentlichung	
Adressaten des Dokuments:	ovag Netz GmbH
Dokumentenverantwortlich/eigentümer:	Axel Finkeldey
Status:	In Kraft
Archivierung bis:	Überarbeitung (aber mind. 6 Jahre)
Speicherort:	P:\ISMS-Projekte\ISMS ovagNetzAG\RL in Kraft

Freigabevermerk:

Datum: 01.11.2019

Peter-Hans Hög

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Die Geschäftsführung der ovag Netz GmbH hat beschlossen ein Managementsystem für Informationssicherheit zu etablieren. Die in diesem Dokument beschriebene Leitlinie für ein Informationssicherheit definiert die grundlegenden Ziele, Strategien und den Rahmen zur Gewährleistung der Informationssicherheit innerhalb der ovag Netz GmbH. Dabei werden die Maßgaben der ISO/IEC 27001:2013, der ISO/IEC TR 27019:2013 und des IT-Sicherheitskatalogs gem. §11 Abs. 1a EnWG umgesetzt.

1.1 Zielsetzung

Die ovag-Gruppe befindet sich über die Gesellschaften ZOV und OVVG in kommunalem Eigentum der Landkreise Wetteraukreis, Vogelsbergkreis und des Landkreises Gießen. Der Unternehmensverbund bündelt die Einzelunternehmen

- Oberhessische Versorgungsbetriebe AG (OVAG)
- ovag Netz GmbH
- Verkehrsgesellschaft Oberhessen mbH (VGO)

Die Geschäftstätigkeit der ovag Netz GmbH umfasst die Planung, die Errichtung, den Betrieb, die Wartung und Unterhaltung sowie den Ausbau und die Nutzung von Netzanlagen und Verteilungsanlagen für Strom einschließlich der Erbringung und Vermarktung dazugehöriger Aufgaben und Dienstleistungen.

Auf Grund der Verabschiedung des IT-Sicherheitskataloges nach §11(1a) EnWG ist die ovag Netz GmbH in der Pflicht ein Informationssicherheitsmanagementsystem (ISMS) einzuführen und zertifizieren zu lassen.

Das ISMS verfolgt das Ziel, jede im Unternehmen verwendete Information angemessen nach ihrem Schutzbedarf abzusichern.

Grundlage hierfür ist ein angestrebtes Sicherheitsniveau auf Basis eines risikobasierten und wirtschaftlich angemessenen Vorgehens. Dabei werden interne und externe sowie regulatorische und gesetzliche Vorgaben berücksichtigt.

Um dieses Ziel zu erreichen und um seiner Verantwortung und den gesetzlichen Vorgaben gerecht zu werden etabliert die Geschäftsführung der ovag Netz GmbH mit dieser Leitlinie eine Informationssicherheitsorganisation und stellt alle benötigten Ressourcen bereit. Dabei werden die Vorgaben der ISO/IEC 27001:2013, der ISO/IEC TR 27019:2013 und gesetzlicher Vorgaben wie durch das IT Sicherheitsgesetz und den IT-Sicherheitskatalog, sowie Informationen aus Gremien wie dem UP KRITIS Anwendung finden.

1.2 ISMS-Ziele

Neben den übergeordneten Zielen des ISMS die Wahrung der Schutzziele der Informationen Vertraulichkeit, Integrität, Verbindlichkeit und Verfügbarkeit zu gewährleisten, formuliert die Geschäftsführung im Rahmen des Management-Reviews weitere Ziele der Managementebene und der operativen Ebene.

Die Erfüllung der Ziele wird anhand von entsprechenden Kennzahlen überwacht. Eine ggf. notwendige Anpassung der Ziele erfolgt im jeweils nächstfolgenden Managementreview.

1.3 Kontext

Das ISMS der ovag Netz GmbH nimmt interne und externe Vorgaben auf und transportiert diese in den betrieblichen Kontext. So werden gesetzliche und regulatorische Anforderungen, z.B. aus dem IT-Sicherheitsgesetz, dem EnWG oder der ARegV, aber auch unternehmerische, wie sie im Rahmen von Konzernvorgaben oder dem Unternehmensleitbild entstehen, aufbereitet und innerhalb des Richtlinienwerkes an den Gegebenheiten in der ovag Netz GmbH gespiegelt und umgesetzt.

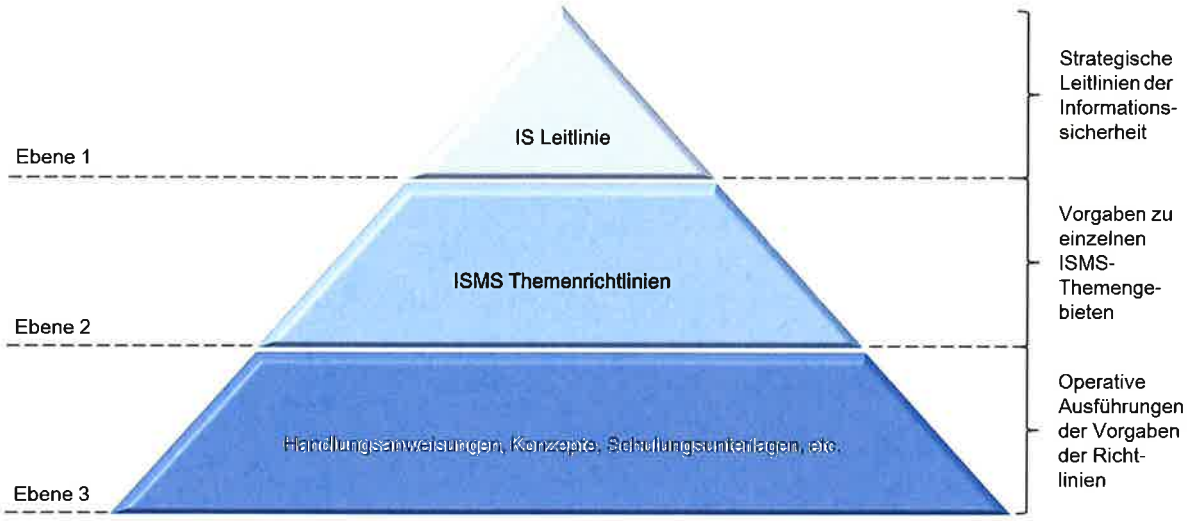

Abbildung 1: Dokumentenebenen

Die Regelungen und Vorgaben des ISMS sind in drei Ebenen gegliedert, wie in Abbildung 1 dargestellt. Die IS Leitlinie setzt dabei die strategischen Leitplanken für den Aufbau und Betrieb eines ISMS innerhalb der ovag Netz GmbH. Die ISMS Themenrichtlinien führen die Vorgaben der IS Leitlinie zu den einzelnen Themengebieten des ISMS weiter aus. Hierbei ist darauf zu achten, dass den Vorgaben dieser Richtlinien auch Verantwortlichkeiten zugeordnet werden. Auf der dritten Ebene entstehen Handlungsanweisungen, Konzepte und weitere Dokumente, dort wo sie entweder von den Richtlinien gefordert werden oder diese für die operative Umsetzung der Vorgaben einer Richtlinie hilfreich sind.

1.4 Anwendungsbereich und Gültigkeit

Mit Beschluss der Geschäftsführung der ovag Netz GmbH wird ein ISMS eingeführt, das die Vorgaben der ISO/IEC 27001:2013, der ISO/IEC TR 27019:2013 und des IT-Sicherheitskatalogs nach §11 Abs. 1a EnWG erfüllt. Die Beschreibung des Anwendungsbereichs findet sich im Dokument „Anwendungsbereich des ISMS“. Die durch die IS Leitlinie legitimierten Richtlinien sind für alle Mitarbeiterinnen und Mitarbeiter innerhalb des Anwendungsbereichs des ISMS der ovag Netz GmbH verbindlich.

1.5 Zielgruppe

Diese IS Leitlinie definiert den Auftrag der Geschäftsführung an die Sicherheitsorganisation ein unternehmensspezifisches und normkonformes ISMS unter Berücksichtigung der Risiken innerhalb der gesamten ovag Netz GmbH zu konzipieren, einzuführen, zu überwachen und kontinuierlich zu verbessern.

1.6 Dokumentenversion

Dieses Dokument ist in der Version 1.1 vom 01.11.2019 gültig und wird, sofern erforderlich, jährlich auf Veranlassung des ISMS Beauftragten überarbeitet.

1.7 Ansprechpartner

Axel Finkeldey, ISMS Beauftragter

Tel.: 06031 / 82-1788

E-Mail: finkeldey@ovag-netz.de

2 Handlungsfelder der Informationssicherheit

Die Geschäftsführung der ovag Netz GmbH hat wesentliche Handlungsfelder der Informationssicherheit identifiziert und stellt die notwendigen Ressourcen dafür im Rahmen des ISMS zur Verfügung. Diese Handlungsfelder werden in den folgenden Abschnitten dargestellt.

2.1 Informationssicherheits-Lenkung

2.1.1 Informationelles Risikomanagement

Die informationellen Risiken der ovag Netz GmbH werden mit Hilfe einer qualitativen Risikoanalyse ermittelt. In diesem Rahmen werden alle Risiken identifiziert, analysiert, bewertet und behandelt, die mit dem Verlust der Vertraulichkeit, Integrität, Verbindlichkeit und Verfügbarkeit einhergehen. Am Ende dieses Prozesses steht dann eine qualitative Aussage über die Sicherheit in der Informationsverarbeitung der unterstützenden Werte im Anwendungsbereich des ISMS, die in das allgemeine Risikomanagement der ovag Netz GmbH einfließt.

Die Risikoanalyse wird bei Änderungen im Anwendungsbereich, mindestens aber einmal im Jahr durchgeführt und das Ergebnis der Geschäftsführung vorgestellt. Zur Behandlung der erkannten Risiken werden Maßnahmen entwickelt, umgesetzt und überwacht, um zu gewährleisten, dass sich die Risikolage der ovag Netz innerhalb der Kriterien für ein akzeptables Risikoniveau befindet, die von der Geschäftsführung definiert wurden.

2.1.2 Internes Kontrollsystem

Die Sicherheitsorganisation des ISMS wird ein internes Kontrollsystem etablieren, in dem mittels geeigneter Kennzahlen gemäß ISO/IEC 27001:2013 der Zustand des ISMS in regelmäßigen Abständen erhoben wird. Die erhobenen Kennzahlen fließen in die Aktivitäten des kontinuierlichen Verbesserungsprozesses ein.

Alle Dokumente des ISMS, einschließlich dieser IS Leitlinie, werden mindestens einmal im Jahr oder bei grundlegenden Veränderungen der internen und externen Gegebenheiten auf Aktualität überprüft und ggf. geeignet angepasst.

2.1.3 Kontinuierlicher Verbesserungsprozess

Das ISMS der ovag Netz GmbH soll kontinuierlich weiterentwickelt werden. Im Rahmen dieses Verbesserungsprozesses wird der Zustand des ISMS überwacht. Aus Abweichungen zu den Vorgaben des ISMS und den erhobenen Kennzahlen werden Verbesserungsmaßnahmen abgeleitet und umgesetzt. Dadurch wird gewährleistet, dass Abweichungen und Schwächen des ISMS über die Zeit nach und nach behoben werden.

2.1.4 Management Review

Der ISMS Beauftragte erstattet der Geschäftsführung der ovag Netz GmbH halbjährlich Bericht über den Zustand des ISMS und die im kontinuierlichen Verbesserungsprozess entwickelten Verbesserungsmaßnahmen. Einer dieser Termine im Jahr wird als Management Review nach ISO/IEC 27001:2013 genutzt.

2.2 IS Vorfallmanagement

Für ein funktionierendes ISMS müssen Informationssicherheitsvorfälle rechtzeitig erkannt und angemessen behandelt werden. Dazu wird ein Informationssicherheitsvorfallmanagement (IS Vorfallmanagement) etabliert, das eine zentrale Meldestelle für die Meldung von Vorfällen durch alle Mitarbeiterinnen und Mitarbeiter beinhaltet. Meldungen erfolgen entweder telefonisch unter **06031 / 82-19040** oder per E-Mail unter **informationssicherheit@ovag-netz.de**.

2.3 Notfall- und Krisenmanagement

Als Eskalationsstufe für das IS Vorfallmanagement hat die ovag Netz ein Notfall- und Krisenmanagement aufgebaut. Mit den dort entwickelten Strukturen und Verfahrensweisen kann die Handlungsfähigkeit der ovag Netz auch im Not- oder Krisenfall gewährleistet werden.

2.4 Bewusstsein (Awareness)

Neben den technischen Maßnahmen zur Absicherung, insbesondere der IT-Systeme, ist das Verhalten und Handeln der Mitarbeiterinnen und Mitarbeiter der ovag Netz GmbH von entscheidender Bedeutung für die Informationssicherheit. Daher werden alle Mitarbeiterinnen und Mitarbeiter entsprechend ihrer Aufgaben in den Inhalten des ISMS geschult. Dazu wird ein entsprechendes Schulungsprogramm entwickelt.

3 Rollen und Verantwortlichkeiten der Informationssicherheit

3.1 Geschäftsführung der ovag Netz GmbH

Die Geschäftsführung der ovag Netz GmbH trägt die Gesamtverantwortung für das ISMS der ovag Netz GmbH. Mit der Verabschiedung dieser IS Leitlinie macht die Geschäftsführung deutlich, wie wichtig das Thema Informationssicherheit für den wirtschaftlichen Erfolg der ovag Netz GmbH und die Versorgungssicherheit der Kunden ist. Um das notwendige Niveau an Informationssicherheit zu gewährleisten stellt die Geschäftsführung alle notwendigen Ressourcen bereit. Die Geschäftsführung überwacht das ISMS regelmäßig, u.a. im Rahmen der Management Reviews.

3.2 ISMS Beauftragter

Der ISMS Beauftragte ist innerhalb der ovag Netz die grundlegende Managementposition, die für Aufbau, Betrieb und Pflege des ISMS verantwortlich ist. Der ISMS Beauftragte hat einen direkten Berichtsweg zur Geschäftsführung der ovag Netz.

Er koordiniert Pläne und Aktivitäten, um die Anforderungen zu erfüllen, die sich aus der IS Leitlinie und daraus abgeleiteten Dokumenten ergeben. Er ist verantwortlich für die Strukturierung der Inhalte und die Pflege dieser Dokumente. Weiterhin obliegt ihm die Bereitstellung von Verfahren und Methoden im Bereich der Informationssicherheit, z.B. für die Erstellung von Sicherheitskonzepten, die Durchführung von Risikoanalysen oder Security Reviews.

3.3 Ansprechpartner IT-Sicherheit nach IT Sicherheitskatalog gemäß §11 Abs. 1a EnWG

Der Ansprechpartner IT Sicherheit stellt die Kontaktstelle für die Bundesnetzagentur dar, wie diese im IT Sicherheitskatalog nach EnWG §11 Abs. 1a gefordert ist. Er ist Ansprechpartner für alle Fragen rund um den Umsetzungsstand des ISMS und ggf. aufgetretener Informationssicherheitsvorfälle.

3.4 Informationssicherheitsmanagementteam (ISMT)

Das ISMT wird dazu genutzt, um über Fragen der Informationssicherheit zu diskutieren. In diesem Gremium werden Maßnahmen zur Umsetzung der Anforderungen des ISMS der ovag Netz GmbH entwickelt und beraten. Es werden Themenrichtlinien erarbeitet und verabschiedet.

3.5 Alle Mitarbeiter

Alle Mitarbeiter im Anwendungsbereich des ISMS der ovag Netz GmbH sind dazu verpflichtet die Vorgaben der Informationssicherheit zu befolgen.