SWE Erfurt Netz

ISMS

Leitlinie zur Informationssicherheit SWE Netz GmbH

Anwendungsbereich:
SWE Netz GmbH · Magdeburger Allee 34 · 99086 Erfurt

Änderungsverzeichnis

Datum	Bearbeiter	Änderungsgrund	Version
03.12.2018	ISB	Erstfassung	1.0

Informationen zum Dokument

Dokumentstatus:	Final		
Dokumentversion:	1.0 vom 03.12.2018		
Vertraulichkeitsklasse	Offen		
Ablage:			
Dokumentverantwortlicher:	Informationssicherheitsbeauftragter		
Prüfung		am	

Inhalt

1 Einleitung

Die SWE Netz GmbH ist ein Unternehmen der Stadtwerke Erfurt Gruppe. Zum Leistungsspektrum der Stadtwerke Erfurt Netz GmbH gehören die Versorgung mit Strom und Gas. Als Netzbetreiber in Erfurt ist die SWE Netz GmbH verantwortlich für das Halten, den Betrieb, die Wartung und den Ausbau verschiedener für die Energieversorgung in Erfurt erforderlichen Netze und Anlagen. Sie nimmt die Tätigkeit eines Netzbetreibers im Sinne des § 3 Ziffer 4 EnWG wahr.

Der Bereich der Energieversorgung gehört zu den kritischen Infrastrukturen, deren Schutz von hoher Bedeutung ist. Kritische Infrastrukturen werden in hohem Maße durch Informationstechnologien gesteuert und kontrolliert. Die Informationstechnologie spielt somit eine wesentliche Rolle für die Aufgabenerfüllung der SWE Netz GmbH. Durch diese verstärkte Abhängigkeit hat sich das Risiko der Beeinträchtigung von Informationsinfrastrukturen und deren Komponenten durch vorsätzliche Angriffe von innen und außen, durch fahrlässiges Handeln, Unkenntnis oder potenzielles Versagen der Technik, sowohl qualitativ als auch quantitativ deutlich erhöht.

Die Geschäftsführung der SWE Netz GmbH hat beschlossen, ein Informationssicherheitsmanagement-system (ISMS) zu etablieren. Die in diesem Dokument beschriebene Informationssicherheitspolitik der SWE Netz GmbH definiert die grundlegenden Ziele, Strategien und den Rahmen zur Gewährleistung der Informationssicherheit im Unternehmen.

2 Gegenstand und Geltungsbereich

Die vorliegende Informationssicherheits-Leitlinie beschreibt die allgemeinen Ziele, Organisationsstrukturen und Maßnahmen, welche für die Entwicklung, die Implementierung, das Betreiben sowie Überwachen und Aufrechterhalten eines Informationssicherheits-Managementsystems (ISMS) erforderlich sind.

Es dient allen internen wie externen Mitarbeitern sowie Vertragspartnern und allen weiteren interessierten Dritten als Orientierung hinsichtlich der Aktivitäten bezüglich der Informationssicherheit und ist verbindliche Grundlage für alle ISMS-Aktivitäten im Unternehmen.

Die Inhalte dieser Leitlinie sind verbindliche für alle internen Mitarbeiter der SWE Netz GmbH. Darüber hinaus sind sie verbindliche Grundlage für alle Externen, die

- an Geschäftsprozessen der SWE Netz GmbH teilnehmen,
- Geschäftsprozesse der SWE Netz GmbH als Dienstleistung ausführen
- auf interne Informationen zugreifen,
- Zugang zu internen IT-Systemen bekommen,
- Zutritt zu Räumlichkeiten mit Bezug zu Informationen oder der Informationsverarbeitung haben.

3 Ziele der Informationssicherheit

Die Geschäftstätigkeit der SWE Netz GmbH ist in hohem Maße von IT- und Kommunikationstechnik abhängig und somit essentiell für die Geschäftstätigkeit des Unternehmens. Insbesondere für Netzbetreiber ist die Gewährleistung einer hohen Informationssicherheit von beträchtlicher Bedeutung, um den Betrieb eines sicheren und zuverlässigen Energieversorgungsnetzes sicherzustellen.

Mit der Einführung eines Informationssicherheitsmanagementsystems (ISMS) werden deshalb folgende Informationssicherheitsziele verfolgt und umgesetzt:

- Schutz von Informationen und IT-Systeme gegen unbeabsichtigte Veränderung, vorsätzliche Verfälschung und Beschädigungen/Diebstahl
- Gewährleistung von stets aktuellen, vollständigen und sicheren Informationen in allen IT- und Kommunikationsverfahren - Fehlfunktionen und Unregelmäßigkeiten in Daten und IT-Systemen sind nur in geringem Umfang und nur in Ausnahmefällen akzeptabel.
- Sicherstellung, dass die IT- und Kommunikationsverfahren eine Übermittlung von Informationen bzw. der Zugriff auf Informationen an bzw. durch unberechtigte Dritte nicht zulassen

Neben den dabei zu erfüllenden Anforderungen an die Informationssicherheit zur Aufrechterhaltung des Geschäftsbetriebes unterliegt die SWE Netz GmbH gesetzlichen, behördlichen sowie vertraglichen Vorgaben, welche einzuhalten sind:

- Schutz der an die SWE Netz GmbH übermittelten Informationen vor dem Zugriff und der Einsichtnahme durch unberechtigte Personen
- zuverlässige und sichere Erbringung der vertraglich vereinbarten Leistungen
- Umsetzung und Einhaltung von behördlichen Vorgaben und Gesetzen, insbesondere das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), die Regelungen des Gesetzes über die Elektrizitäts- und Gasversorgung (EnWG), das Bundesdatenschutzgesetz und den „IT-Sicherheitskatalog“ der Bundesnetzagentur

Entsprechend den eigenen Anforderungen sowie den Erfordernissen und Erwartungen von Kunden, Partnern und Behörden ist es das Ziel der Informationssicherheit, die Verfügbarkeit von Informationen bzw. der Systeme, mit denen diese verarbeitet werden, so zu schützen, so dass die **Vertraulichkeit**, die **Integrität** sowie die **Verfügbarkeit** in einem dem jeweiligen Stellenwert der Informationen angemessenen Maß gesichert sind.

Alle Beteiligten (Kunden, Dienstleister, Lieferanten, Partner, Gesellschafter, etc.) müssen sich darauf verlassen können, dass die SWE Netz GmbH die Sicherheitsverantwortung für die von ihr verarbeiteten Informationen gewissenhaft wahrnimmt und vor missbräuchlicher Verwendung schützt. Die Daten und die IT-Anwendungen werden daher einem hohen Vertraulichkeitsschutz unterzogen.

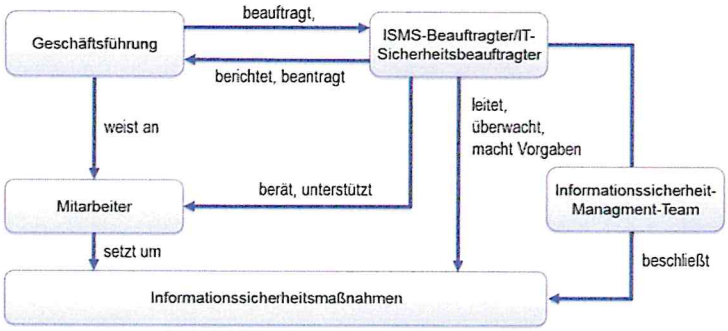
Alle Mitarbeiterinnen und Mitarbeiter der SWE Netz GmbH halten die in ihrer Tätigkeit zu beachtenden einschlägigen gesetzlichen Regelungen (insbesondere datenschutzrechtliche und informationssicherheitsrelevante) sowie betriebliche Anweisungen und vertragliche Regelungen ein. Negative finanzielle und immaterielle Folgen für das Unternehmen sowie für die Mitarbeiter durch Gesetzesverstöße sind zu vermeiden.

Alle Mitarbeiter sowie die Geschäftsführung sind sich ihrer Verantwortung beim Umgang mit Informationen und Informationstechnik bewusst und unterstützen die Integration eines Informationssicherheits-Managementsystems in die Unternehmensprozesse sowie die Informationssicherheitsstrategie nach besten Kräften.

Um den Anforderungen des § 11 Absatz 1a EnWG, aber auch eigenen Sicherheitszielen und den Anforderungen der Bevölkerung hinsichtlich einer sicheren Strom- und Gasversorgung zu genügen sowie zum Schutz ihrer Informationen und informationsverarbeitenden Systeme, betreibt die SWE Netz GmbH ein ISMS nach ISO/IEC 27001:2013 für den Anwendungsbereich „IKT-Systeme für den sicheren Netzbetrieb".

4 Organisation der Informationssicherheit

Die Geschäftsführung der SWE Netz GmbH trägt Gesamtverantwortung für die Informationen und IT-Systeme des Unternehmens und übernimmt die Gesamtverantwortung für die Informationssicherheit im Unternehmen. Zur Erreichung der Informationssicherheitsziele wird eine Informationssicherheitsorganisation eingerichtet. (siehe Abbildung)



Es ist ein zentraler Informationssicherheitsbeauftragter (ISB) benannt. Der Informationssicherheitsbeauftragte initiiert, steuert und kontrolliert unter Beteiligung des Informationssicherheitsmanagementteams (IS-MT) den Informationssicherheitsprozess und veranlasst bei Notwendigkeit unverzüglich die erforderlichen Maßnahmen zur Gewährleistung der Informationssicherheit.

Der Informationssicherheitsbeauftragte der SWE Gruppe übernimmt die Aufgaben des Informationssicherheitsbeauftragten und des ISMS-Beauftragten der SWE Netz GmbH. Außerdem ist er der Ansprechpartner „IT-Sicherheit" gegenüber der BNetzA.

Dem Informationssicherheits-Management-Team gehören folgende Personen an:

- CIO der Stadtwerke Erfurt GmbH,
- der Informationssicherheitsbeauftragte der SWE Gruppe,
- der Datenschutzbeauftragte der Stadtwerke Erfurt GmbH,
- Verantwortlicher IT Infrastruktur des IT-Dienstleisters,
- IT-Management und Leittechnik der SWE Netz (bei zuständigen Themen)
- sowie bei Bedarf weitere Ansprechpartner.

5 Maßnahmen zum Schutz der Informationssicherheit

Um die Informationssicherheit für alle Informationen und Daten, die von der SWE Netz verarbeitet werden sicherzustellen sind entsprechende Sicherheitsmaßnahmen festgelegt und umgesetzt:

- Für alle Verfahren, Informationen, IT-Anwendungen und IT-Systeme ist eine verantwortliche Person benannt, die den Informationssicherheitsbeauftragten bei der Feststellung des Schutzbedarfs unterstützt. Auf dieser Grundlage werden konkrete Schutzmaßnahmen zur Sicherstellung der geforderten Vertraulichkeit, Verfügbarkeit und Integrität festgelegt.

- Für alle verantwortlichen Funktionen sind Vertretungen eingerichtet, durch Unterweisungen und ausreichende Dokumentationen wird sichergestellt, dass Vertreter ihre Aufgaben erfüllen können.

- Alle erhobenen, gespeicherten, verarbeiteten und weitergegebenen Daten werden vertraulich behandelt und jederzeit vor unbefugtem Zugriff geschützt. Der Zugriff auf IT-Systeme, IT-Anwendungen und Daten sowie Informationen ist auf den unbedingt erforderlichen Personenkreis beschränkt.

- Gebäude und Räumlichkeiten werden durch ausreichende Sicherheitsmaßnahmen gegen unbefugten Zutritt geschützt. Der Zugang zu IT-Systemen und IT-Anwendungen wird durch angemessene Zugangskontrollen und der Zugriff auf die Daten durch ein restriktives Berechtigungskonzept geschützt.

- Die Funktionssicherheit der Serverräume (u.a. Klimatisierung, Sicherheitstechnik, Energieversorgung) wird als wesentliches Sicherheitsziel bei der Entwicklung der IT-Systeme und -Strukturen berücksichtigt, die entsprechende Technik wird bedarfsgerecht qualifiziert.

- Computer-Viren-Schutzprogramme werden auf allen IT-Systemen eingesetzt. Alle Internetzugänge werden durch eine geeignete Firewall gesichert. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen verhindert werden.

- Die IT-Benutzer unterstützen durch eine sicherheitsbewusste Arbeitsweise die Sicherheitsmaßnahmen und informieren bei Auffälligkeiten den Informationssicherheitsbeauftragten der SWE Netz GmbH.

- Durch eine umfassende Datensicherung wird gewährleistet, dass der IT-Betrieb bei Störungen oder Datenverlust kurzfristig wiederaufgenommen werden kann.

- Um größere Schäden in Folge von Notfällen zu begrenzen bzw. diesen vorzubeugen, wird auf sicherheitsrelevante Vorfälle zügig und konsequent reagiert– entsprechende Maßnahmen sind in einem Notfallhandbuch zusammengestellt.

- Personen und Unternehmen, die nicht zu der SWE Netz GmbH gehören, für diese aber Leistungen erbringen, werden zur Einhaltung der Vorgaben zur Informationssicherheit der SWE Netz GmbH verpflichtet.

- Sofern IT-Dienstleistungen an externe Stellen ausgelagert werden, werden konkrete Sicherheitsanforderungen vorgegeben und das Recht auf Kontrolle wird festgelegt.
- Ein Prozess für den Umgang mit Informationssicherheitsrisiken ist definiert und die Methodik zur Einschätzung und Behandlung von Informationssicherheitsrisiken ist festgelegt. Auf Basis der Analyse und Bewertung der Informationssicherheitsrisiken werden angemessene Maßnahmen zum Schutz von Informationssystemen definiert, umgesetzt und fortwährend geprüft und angepasst.

Die oben genannten Sicherheitsmaßnahmen werden in separaten Richtlinien und Dienstanweisungen weiter konkretisiert und bilden damit die Grundlage für eine sichere und ordnungsgemäße Nutzung der IT-Technik in der SWE Netz GmbH.

6 Verbesserung der Informationssicherheit

Die Maßnahmen zur Informationssicherheit werden regelmäßig auf Aktualität und Wirksamkeit geprüft.

Die Geschäftsführung unterstützt die ständige Verbesserung des Sicherheitsniveaus. Mitarbeiter sind angehalten, mögliche Verbesserungen oder Schwachstellen an die entsprechenden Stellen (Informationssicherheitsbeauftragter der SWE Netz GmbH) weiterzugeben.

Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheits- und Datenschutzniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, die Informationssicherheitssituation zu verbessern und ständig auf dem aktuellen Stand der Informationssicherheit zu halten.

Durch Schulungs- und Sensibilisierungsmaßnahmen werden die Voraussetzungen geschaffen, dass sich alle Mitarbeiter der SWE Netz GmbH Ihrer Verantwortung für die Umsetzung der Informationssicherheitsmaßnahmen bewusst sind.

Erfurt, den 8.1.2019

SWE Netz GmbH

Heidemann

Frank Heidemann

Geschäftsführer