Zielgruppe

Alle Mitarbeiter der EnR Energienetze Rudolstadt GmbH (EnR).

Klassifikation

Dieses Dokument wurde als öffentlich eingestuft.

Änderungshistorie

Ver-sion	Modifikation	Datum	Typ	Verantwortlich
0.1	Erster Entwurf	05.11.2025	Bearbeitung	Christian Gerlach
1.0	Freigabe	06.11.2025		Alf-Dieter Borsch
0.3	Dritter Entwurf	04.01.2017	Bearbeitung	Lea Simon, Stefan Krähmer
1.0	Freigabe	27.07.2017		Alf Borsch
1.0	Review	05.11.2018		Alf Borsch
1.0	Review	10.11.2019		Alf Borsch
1.0	Review des Doku-mentes	09.11.2020	Prüfung	Hr. Borsch
2.0	Review	19.08.2022	Bearbeitung, Freigabe	Hr. Borsch
2.0	Review	25.07.2024	Prüfung/ Durchsicht	Alf Borsch
2.1	Review	30.10.2025	Überarbeitung	Christian Gerlach
3.0	Freigabe	06.11.2025		Alf Borsch

1 Ziel

Ziel der Informationssicherheit ist es, den Geschäftsbetrieb sicherzustellen und das Risiko eines Schadens durch die Verhütung von Sicherheitsvorfällen und die Reduzierung ihrer potenziellen Auswirkungen zu minimieren. Ziel ist es auch, alle personenbezogenen Informationen gegen alle internen, externen, absichtlichen oder versehentlichen Bedrohungen zu schützen. Aus diesem Grund wurde ein Informationssicherheitsmanagementsystem (ISMS) etabliert, welches regelmäßig auf Wirksamkeit und Angemessenheit überprüft wird.

Durch diese Informationssicherheitspolitik übernimmt die Geschäftsleitung die Gesamtverantwortung.

2 Stellenwert der Informationssicherheit

Die erfolgreiche Planung, Implementierung und Betreuung von IT-Infrastrukturen und komplexen Projekten für Kunden impliziert einen schnellen, sicheren und aktuellen Zugriff auf Informationen, von dem der Erfolg unseres Unternehmens abhängt. Ein Missbrauch dieser Informationen schadet nicht nur dem Ansehen und unserer Reputation, sondern kann auch rechtliche Folgen und Schadensersatzansprüche verursachen. Demzufolge ist dieser Missbrauch zu verhindern.

Eine funktionsfähige Informationstechnik und ein sicherheitsbewusster Umgang mit ihr sind wesentliche Voraussetzungen für unsere täglichen Arbeitsabläufe, das Vertrauen unserer Kunden und Geschäftspartner.

3 Sicherheitsziele und Kernelemente der Sicherheitsstrategie

Um dieses Ziel zu erreichen, soll sichergestellt werden, dass die folgenden Aspekte zur Informationssicherheit erreicht werden:

- Schutz von Informationen gegen alle nicht autorisierten Zugriffe,
- Gewährleisten der Vertraulichkeit der Informationen,
- Gewährleisten der Integrität von Informationen,
- Gewährleisten der Verfügbarkeit von Informationen,
- Gewährleistung von Authentizität von Informationen iSd. § 8a I BSIG,
- Erfüllen von informationssicherheitsrelevanten legislativen und behördlichen Auflagen,
- Entwickeln, Verwalten und Testen von Notfallplänen,
- Anbieten und Durchführen von informationssicherheitsbewusstseinsbildenden Maßnahmen sowie Datenschutzschulungen für alle Mitarbeiter,
- Melden und Untersuchen von tatsächlichen oder vermuteten Informationssicherheitsverletzungen an das ISMS-Team,
- Melden und Untersuchen von tatsächlichen oder vermuteten Datenschutzverletzungen an den Datenschutzbeauftragten.

4 Organisationsstruktur

Zur Erreichung der Sicherheitsziele wird ein Informationssicherheitsbeauftragter (kurz „ISB“) und ein ISMS-Team bestellt. Der ISB und das ISMS-Team sind für die Erstellung und Fortschreibung des Sicherheitskonzepts sowie die Aufrechterhaltung des Sicherheitsniveaus verantwortlich. Sie berichten in ihrer Funktion direkt der Geschäftsleitung.

Dem ISMS-Team werden von der Geschäftsleitung ausreichende finanzielle und zeitliche Ressourcen für die Ausübung ihrer Tätigkeiten zur Verfügung gestellt. Das ISMS-Team ist durch die Geschäftsleitung sowie durch die Mitarbeiter ausreichend zu unterstützen und frühzeitig in alle Projekte einzubinden, um schon in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen. Gleiches gilt, sofern personenbezogene Daten betroffen sind. Die Mitarbeiter haben sich in sicherheitsrelevanten Fragestellungen an die Anweisungen des ISMS-Teams zu halten. Der Datenschutzbeauftragte (kurz „DSB“) steht dem ISMS-Team beratend zur Verfügung.

Das ISMS-Team ist verantwortlich für:

- die Eskalation etwaiger Risiken an die Geschäftsleitung,
- die Beratung der Mitarbeiter zu Fragen zur Informationssicherheit,
- die Schulung der Mitarbeiter in Bezug auf die Informationssicherheit.

5 Rollenzuordnung

Die relevanten Rollen sind in der ISMS-Organisationsstruktur näher beschrieben.

6 Verantwortung der Mitarbeiter

Jeder Mitarbeiter verpflichtet sich, sorgfältig mit den ihm zur Verfügung stehenden Informationen umzugehen und die Leit- und Richtlinien einzuhalten. Eine grobfahrlässige Verletzung der Informationssicherheit kann zu disziplinarischen oder arbeitsrechtlichen Konsequenzen, straf- und zivilrechtlichen Verfahren oder Haftungs- und Regressforderungen führen.

Als grobfahrlässige Verletzungen bzw. Handlungen gelten:

- eine Kompromittierung des Rufes unseres Unternehmens
- eine Bedrohung für die Sicherheit der Mitarbeiter und Dienstleister sowie des Vermögens unseres Unternehmens
- die Gefährdung der Sicherheit von Informationen hinsichtlich deren Verfügbarkeit, Integrität und Vertraulichkeit
- die Kompromittierung der Sicherheit von Daten oder Geschäftsinformationen unseres Unternehmens, welche zu einem tatsächlichen oder potenziellen finanziellen Verlust führt
- der unberechtigte Zugriff auf Informationen, deren Preisgabe und/oder Änderung

- die Nutzung von Unternehmensinformationen für illegale Zwecke

Fahrlässige und vorsätzliche Verstöße gegen die Vorgaben können disziplinarische wie arbeitsrechtliche Schritte nach sich ziehen.

7 Unterstützende Richtlinien und Anweisungen

Das ISMS umfasst neben dieser Politik weitere, verbindliche Richtlinien, Verfahrensanweisungen, Prozesse und betriebliche Dokumentationen. Diese sind im Dateisystem veröffentlicht und sind dort für alle Mitarbeiter jederzeit einsehbar.

Gesetzliche Anforderungen und vertragliche Anforderungen sind von allen Mitarbeitern einzuhalten.

Energienetze Rudolstadt GmbH
Digital unterschrieben von Alf-Dieter Borsch
Datum: 2025.11.10 09:42:43 +01'00'

Geschäftsführung