GGEW
WIR SIND ENERGIE.

Leitlinie

GGEW, Gruppen-Gas- und Elektrizitätswerk Bergstraße AG

"Informationssicherheits-Management"

1. Inhaltsverzeichnis

1. INHALTSVERZEICHNIS 2
2. TABELLENVERZEICHNIS 2
3. DOKUMENTENLENKUNG 3
3.1. DOKUMENTHISTORIE 3
3.2. FREIGABEELEMENTE 3
3.3. GELTUNGSBEREICH UND -AUSSCHLÜSSE 3
3.4. GELTUNGSZEIT 3
3.5. KLASSIFIKATION 3
4. ALLGEMEINES 4
4.1. ZWECK 4
5. STELLENWERT DER INFORMATIONSSICHERHEIT 4
5.1. IT IST UNVERZICHTBARE BASIS DER GESCHÄFTSPROZESSE 4
5.2. ERFÜLLUNG GESETZLICHER UND VERTRAGLICHER VERPFLICHTUNGEN 4
5.3. BEDEUTUNG DER INFORMATIONSSICHERHEIT 4
5.4. HERKUNFT DER LEITLINIEN 4
6. INFORMATIONSSICHERHEITSZIELE UND SCHUTZMAßNAHMEN 5
7. ORGANISATIONSSTRUKTUR UND VERANTWORTLICHKEITEN 6
7.1. GESCHÄFTSLEITUNG 6
7.2. IT-VERANTWORTLICHER PLT 6
7.3. ISMS-BEAUFTRAGTE 6
7.4. ANSPRECHPARTNER IT-SICHERHEIT 6
7.5. BETRIEBLICHE DATENSCHUTZBEAUFTRAGTE 7
7.6. IT-ADMINISTRATOR PLT 7
7.7. PERSONALVERANTWORTLICHE 7
7.8. MITARBEITER 7
8. SCHULUNGS- UND SENSIBILISIERUNGSMAßNAHMEN 7
9. SANKTIONEN 7
10. KONTINUIERLICHER VERBESSERUNGSPROZESS 8
11. REFERENZDOKUMENTE 8

2. Tabellenverzeichnis

TABELLE 1 DOKUMENTHISTORIE 3
TABELLE 2 DOKUMENTHISTORIE 3

3. Dokumentenlenkung

3.1. Dokumenthistorie

Datum	Autor	Versionsbeschreibung / Änderungen
01.11.2017	Uwe Sänger	Version 1.0
20.12.2017	Uwe Sänger	Version 1.1

Tabelle 1 Dokumenthistorie

3.2. Freigabeelemente

Dokumenten-Verantwortlicher	Freigabestatus	Freigebende Rolle	Freigabedatum	Unterschrift
Uwe Sänger	freigegeben	Vorstand	20.12.2017	

Tabelle 2 Dokumenthistorie

3.3. Geltungsbereich und -ausschlüsse

Diese Leitlinie wird auf das gesamte Informationssicherheits-Managementsystem (ISMS) sowie alle mit diesem in Verbindung stehenden Richtlinien, Prozesse, Verfahren, Pläne und sonstige Dokumentationen angewendet.

Die Leitlinie Informationssicherheits-Management enthält Aufforderung und Verpflichtung zu gesetzeskonformen Verhalten und verantwortungsbewusstem Umgang mit Informationen und der IKT-Infrastruktur des Unternehmens für alle, die diese Infrastruktur nutzen. Sie wird allen Mitarbeitern, Partnern und ggf. weiteren Personen oder Einrichtungen in geeigneter Weise zur Kenntnis gegeben.

3.4. Geltungszeit

Dieses Dokument gilt ab Freigabedatum.

3.5. Klassifikation

öffentlich.

4. Allgemeines

4.1. Zweck

Zielsetzung dieser Leitlinie ist die Definition des Zwecks, der Ausrichtung, der Grundlagen und der grundsätzlichen Regeln für das Informationssicherheits-Management.

5. Stellenwert der Informationssicherheit

5.1. IT ist unverzichtbare Basis der Geschäftsprozesse

Die GGEW, Gruppen-Gas- und Elektrizitätswerk Bergstraße AG, ist als Energiedienstleistungsunternehmen auf die Verfügbarkeit moderner Informations- und Kommunikationstechnik (IKT) angewiesen, um ihre Geschäftsprozesse durchzuführen, die Leistungen für Ihre Kunden zu erbringen, und um mit Kunden und Geschäftspartnern zusammenarbeiten zu können.

5.2. Erfüllung gesetzlicher und vertraglicher Verpflichtungen

Darüber hinaus bestehen Verpflichtungen zur Gewährleistung der IT-Sicherheit aufgrund gesetzlicher Bestimmungen und vertraglicher Verpflichtungen gegenüber Kunden, Mitarbeitern und Projektpartnern.
Für Betreiber von Energieversorgungsnetzen fordert der durch die Bundesnetzagentur veröffentlichte IT-Sicherheitskatalog die Einführung eines ISMS zum Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind.

5.3. Bedeutung der Informationssicherheit

Dem Schutz der Informations- und Kommunikationsinfrastruktur der GGEW AG vor Missbrauch, Manipulation, Störungen sowie dem Schutz der gespeicherten und verarbeiteten Informationen vor Manipulation oder Ausspähen – kurz: der IT- und Informationssicherheit – kommt daher eine für das Unternehmen existentielle Bedeutung zu.

5.4. Herkunft der Leitlinien

Aus diesem Grund hat die Geschäftsführung die nachstehenden Leitlinien für den Umgang mit der Informations- und Kommunikationstechnik beschlossen.

6. Informationssicherheitsziele und Schutzmaßnahmen

Die Ziele der Informationssicherheit sind es einen anhaltenden geschäftlichen Erfolg und einen kontinuierlichen Geschäftsbetrieb
sicherzustellen. Daher erfolgt die Sicherstellung der Informationssicherheit im ureigenen Interesse des Unternehmens aber auch im Sinne von deren Kunden, Mitarbeitern und Geschäftspartnern, kurz allen relevanten Stakeholdern.

Um Beeinträchtigungen der Informationssicherheit zu minimieren ist das Management von angemessenen Sicherheitsmaßnahmen unter Berücksichtigung einer großen Bandbreite von Bedrohungen erforderlich.

- Die GGEW AG schützt ihre eigene Arbeitsfähigkeit, Vertrauenswürdigkeit und Zuverlässigkeit
- Die GGEW AG schützt die Vertraulichkeit der verarbeiteten und gespeicherten Daten ihrer Kunden, Geschäftspartner und Mitarbeiter
- Die GGEW AG schützt vertrauliche Informationen wie z. B. Geschäftsprozesse, Vertragsdaten oder sonstige Geschäftsgeheimnisse
- Die GGEW AG gewährleistet die Verfügbarkeit ihrer IT-Systeme, Programme und Daten
- Die GGEW AG schützt die Integrität ihrer IT-Systeme, Programme und Daten
- Die GGEW AG verhindert den Missbrauch ihrer IT-Systeme, Programme und Daten von zweckwidriger Nutzung, Nutzung durch Unbefugte

Die Schutzmaßnahmen umfassen:

- Technische Maßnahmen (Software, Hardware, Konfiguration)
- Organisatorische Vorkehrungen (verbindliche Regeln und Vorgaben)
- Personelle Maßnahmen (Schulungen, Mitarbeiterauswahl)

Sie werden in

- dem Notfallhandbuch
- verschiedenen Betriebshandbüchern
- Richtlinien
- Dienstanweisungen

hinterlegt und sind zu befolgen.

7. Organisationsstruktur und Verantwortlichkeiten

Das Erreichen, Erhalten und ständige Verbessern eines angemessenen Sicherheitsniveaus erfordert ein kontinuierliches Engagement von allen mit der Informationsverarbeitung befassten Personen wie dem Management, den Nutzern sowie den Administratoren.

7.1. Geschäftsleitung

- Die Geschäftsleitung trägt die Gesamtverantwortung für die Informationssicherheit. Sie initiiert und koordiniert die entsprechenden Aktivitäten und sorgt für die nötige Priorität und Aufmerksamkeit für Fragen der Informationssicherheit. Die Geschäftsleitung ist insbesondere verantwortlich für die organisatorische Verankerung von Aktivitäten zur Etablierung, Erhaltung und Weiterentwicklung der Informationssicherheit sowie für die technische, monetäre und personelle Ressourcen-Ausstattung für die Informationssicherheit und deren angemessene Einbettung in die Strukturen und die Hierarchie der Firma

7.2. IT-Verantwortlicher PLT

- Der IT-Verantwortliche der Prozessleittechnik (PLT) setzt die festgelegten Maßnahmen um und dokumentiert diese.

7.3. ISMS-Beauftragte

- Der ISMS-Beauftragte etabliert das ISMS und entwickelt es weiter. Dabei sorgt er dafür, dass das ISMS in den relevanten Geschäftsprozessen integriert wird und kontrolliert dies. In dem Zuge hat er die Kompetenz, die Änderung der Richtliniendokumente zu initiieren.

- Darüber hinaus legt er diejenigen Maßnahmen fest, die aus seiner Sicht zur Verbesserung und Erhaltung der Sicherheit in dem jeweiligen Wirkungsbereich ergriffen werden müssen; er reagiert außerdem eigenverantwortlich bei Verstößen gegen und bei Nichtbeachtung von Informationssicherheitsvorgaben

7.4. Ansprechpartner IT-Sicherheit

- Dem Ansprechpartner für IT-Sicherheit obliegt gemäß IT-Sicherheitskatalog der BNetzA die Koordination und Kommunikation der IT-Sicherheit gegenüber der Bundesnetzagentur. Im Rahmen dieser Funktion berichtet er auf Anfrage unverzüglich über:

    - Den Umsetzungsstand der Anforderungen aus dem IT-Sicherheitskatalog
    - Aufgetretene Sicherheitsvorfälle sowie Art und Umfang sowie evtl. hierdurch hervorgerufener Auswirkungen
    - Ursache aufgetretener Sicherheitsvorfälle sowie Maßnahmen zu deren Behebung und zukünftigen Vermeidung

  Zudem stellt er sicher, dass der Betreiber geeignet an relevante Kommunikationsinfrastrukturen für Lageberichte und Warnmeldungen sowie zur Bewältigung großflächiger IKT-Krisen angebunden ist.

7.5. Betriebliche Datenschutzbeauftragte

- Der Datenschutzbeauftragte ist das innerbetriebliche Kontrollorgan in allen Datenschutzfragen. Er wirkt auf die Einhaltung der datenschutzrechtlichen Vorschriften hin. Darüber hinaus unterstützt er die Leitung des Unternehmens sowie die Mitarbeiter bei der Identifikation von datenschutzrechtlichen Belangen sowie der Planung und Umsetzung von Maßnahmen zum Datenschutz

7.6. IT-Administrator PLT

- Der Administrator der Prozessleittechnik (PLT) setzt in enger Abstimmung mit dem jeweiligen IT-Verantwortlichen, bzw. Informationssicherheitsbeauftragten die notwendigen technischen und organisatorischen Maßnahmen zur Absicherung der IT-Infrastruktur um. Er erarbeitet konkrete Handlungsanweisungen für die Benutzer der IT-Infrastruktur auch in Bezug auf die IT-Sicherheit und ist aufgefordert, Vorschläge für die Verbesserung der Informationssicherheit an dem Arbeitskreis Informationssicherheit bzw. den IT-Verantwortlichen zu unterbreiten. Die Handlungsanweisungen werden in einem Dokumentenmanagementsystem gesammelt und verwaltet

7.7. Personalverantwortliche

- Die Vorgesetzten mit Personalverantwortung stellen sicher, dass die getroffenen technischen, organisatorischen und personellen Maßnahmen zur Informationssicherheit in Bezug auf die ihnen unterstellten Mitarbeitern bzw. die in ihrem Verantwortungsbereich tätigen Nutzern umgesetzt werden

7.8. Mitarbeiter

- Jeder Mitarbeiter trägt durch sein Verhalten zur Gewährleistung der Informationssicherheit bei. Er wird individuell über die zur Verfügung stehenden Informationssicherheitsmaßnahmen und Mechanismen informiert und achtet darauf, sie konsequent anzuwenden. Zu diesem Zweck erhalten alle betroffenen Mitarbeiter Informationen, Schulung und Betreuung im Umgang mit den IT-Systemen und ihren Sicherheitsmechanismen

8. Schulungs- und Sensibilisierungsmaßnahmen

Die Geschäftsleitung sowie die verantwortlichen Mitarbeiter der GGEW AG stellen sicher, dass neu eingestellte Mitarbeiter ebenso wie bereits beschäftigte Mitarbeiter auf die Einhaltung der Leitlinien hingewiesen werden. In regelmäßigen Abständen (mindestens jährlich) werden die Mitarbeiter auf die Problematiken und Gefährdungen der Informationssicherheit hingewiesen. Mitarbeiter, die direkten Umgang mit sensiblen Informationen haben, werden in internen oder externen Schulungen mit den Gefahren und Maßnahmen der IT-Sicherheit vertraut gemacht.

9. Sanktionen

Die Geschäftsleitung sowie Mitarbeiter mit Personalverantwortung stellen sicher, dass die Leit- und die Richtlinien zur Informationssicherheit durch alle Mitarbeiter befolgt werden. Mitarbeiter, die gegen diese Leit- oder Richtlinien verstoßen, können mit angemessenen Sanktionen belegt werden. Schwerwiegende Verstöße gegen die Grundsätze der Informationssicherheit können zu Abmahnung oder fristloser Kündigung eines Mitarbeiters führen.

10. Kontinuierlicher Verbesserungsprozess

Durch eine kontinuierliche Revision der Einhaltung der Regelungen mittels jährlicher interner Audits und Überwachung wird das angestrebte Informations- bzw. IT-Sicherheits- und Datensicherheitsniveau sichergestellt. Abweichungen müssen mit dem Ziel analysiert werden, die Sicherheitssituation zu verbessern und ständig auf dem aktuellen Stand zu halten um eine kontinuierliche Verbesserung des ISMS sicherzustellen.

Die Informationssicherheit ist ein sich schnell entwickelndes Feld, Die Leitlinie zur Informationssicherheit wird in regelmäßigen Abständen, auf ihre Aktualität und Wirksamkeit hin überprüft und gegebenenfalls angepasst. Im Besonderen wird die Leitlinie bei Änderungen der Bedrohungslage aufgrund aktueller Ereignisse oder der Einführung neuer Technologien in der Firma überprüft und angepasst. Unabhängig davon erfolgt eine Überarbeitung der Leitlinie mindestens einmal im Jahr.

11. Referenzdokumente

- ISO/IEC 27001
- Dokument zum ISMS Anwendungsbereich
- Methodik zur Risikoeinschätzung und Risikobehandlung
- Erklärung zur Anwendbarkeit
- Liste amtlicher, gesetzlicher, vertraglicher und anderer Anforderungen
- Alle internen Dokumente der Organisation, die mit dieser Richtlinie zusammenhängen