Informationssicherheitsleitlinie

Stand 08/2024

Ziel und Zweck dieser Anweisung

Diese Anweisung beschreibt die Organisation der Informationssicherheit bei Gasunie Deutschland (GUD) und die grundsätzliche Politik und Gestaltung des GUD Informationssicherheitsmanagementsystems (ISMS) sowie der zu Grunde liegenden Rahmenbedingungen und Prinzipien.

1. Einleitung

Das Management der GUD verabschiedet hiermit folgende Leitlinie zur Informationssicherheit als Bestandteil ihrer Unternehmensstrategie.

Aufgrund der Weiterentwicklung der Informationstechnik unterliegen diese Informationssicherheitsleitlinie und die darauf aufbauenden Richtlinien einer ständigen Anpassung und Weiterentwicklung. Die Informationssicherheitsleitlinie wird auf Anfrage allen interessierten Parteien der GUD in der jeweils aktuell gültigen Fassung zur Verfügung gestellt.

2. Verpflichtung aller Personen

Die Informationssicherheitsleitline gilt für alle Personen, die Informationen und IT-Services der GUD nutzen und für alle IT-Systeme, die durch oder im Auftrag von GUD betrieben werden. Als IT-Systeme gelten sämtliche IT-Komponenten und IT-Applikationen sowie Telekommunikationssysteme.

3. Informationen und Sicherheit

3.1 Notwendigkeit und Stellenwert der Informationssicherheit

GUD steht für einen sicheren und zuverlässigen Gastransport. Aufgrund seiner besonderen Bedeutung für das Funktionieren des Gemeinwesens stellt ein zuverlässiger Gastransport eine kritische Dienstleistung im Sinne des § 10 Absatz 1 Satz 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik dar.

Für die Sicherstellung des Gastransportes sowie die Ausführung weiterer wesentlicher Geschäftsprozesse ist GUD abhängig von einer funktionsfähigen und sicheren Informationsverarbeitung. Zudem stellen Informationen und Systeme, mit denen Informationen elektronisch verarbeitet werden, einen erheblichen Unternehmenswert dar. Aufgrund der zentralen Bedeutung informationsverarbeitender Systeme für die Geschäftsprozesse und der weltweit steigenden Zahl von Angriffen auf IT-Systeme hat die Informationssicherheit einen sehr hohen Stellenwert bei GUD.

Die Hauptrisiken für die elektronische Informationsverarbeitung bei GUD sind länger anhaltende Ausfälle von geschäftskritischen Systemen, die Gefährdung von geschäftskritischen Systemen und Informationen durch Schadsoftware, Manipulationen oder kriminelle Personen sowie der Diebstahl oder die Verfälschung schützenswerter Informationen. Diese Bedrohungen können zur einer temporären Nichtverfügbarkeit und dem Verlust der technischen Integrität von Systemen führen sowie in einen ernsthaften Datenverlust resultieren. Hierdurch kann die Versorgungssicherheit beeinträchtigt und für GUD ein finanzieller Schaden sowie ein Ansehensverlust in der Öffentlichkeit entstehen.

3.2 Zielsetzung der Informationssicherheit

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

Die Schutzziele sind dabei wie folgt definiert:

- **Vertraulichkeit:** Schutz von Informationen vor nicht genehmigter Preisgabe oder unbefugtem Zugriff
- **Integrität:** Schutz der Informationen und Systeme vor unbeabsichtigter bzw. unerlaubter Veränderung (bis hin zur Löschung und Zerstörung)
- **Verfügbarkeit:** Schutz vor ungeplantem Stillstand der Systeme und Nichtverwendbarkeit der Informationen.

3.3 Grundsätze und Ziele der Informationssicherheit bei der GUD

Das Informationssicherheitsmanagementsystem (ISMS) der GUD folgt den aufgeführten Grundsätzen.

3.3.1 Sensibilisierung

Alle Mitarbeitende und Benutzer von GUD IT-Systemen müssen die Regelungen des ISMS kennen und beachten.

Durch regelmäßige Schulungen und Überprüfungen muss sichergestellt werden, dass das Bewusstsein für Informationssicherheit den erteilten Nutzungsrechten und dem daraus resultierenden Schadenspotential entspricht. Die Verantwortung hierfür liegt bei den einzelnen GUD Fachbereichen

Damit ergibt sich eine persönliche Verantwortung jedes Mitarbeitenden und Benutzer für seine/ihre Handlungen.

3.3.2 Prinzip der „Minimalen Rechte"

Ein wichtiges Grundprinzip der Informationssicherheit ist das "Prinzip der minimalen Rechte". Zugriffsrechte für schützenswerte Informationen und Systeme sind dementsprechend nur in dem Umfang zu gewähren, wie sie zur Aufgabenerfüllung notwendig sind („Need to know, need to do"). Sie dürfen nur durch dafür Befugte erteilt werden und sind in regelmäßigen Abständen zu überprüfen.

3.3.3 Nachvollziehbarkeit

Zugriffe auf schützenswerte Informationen und Systeme müssen nachvollzogen werden können. Die Zugriffskontrollsysteme müssen es daher ermöglichen, die Zugriffsrechte für Benutzer auf Ressourcen anhand von Regeln zu kontrollieren und zu verwalten. Die Identifikation und Authentifikation von Benutzern muss bei allen sicherheitsrelevanten Anwendungen einen eindeutigen Rückschluss auf die Person ermöglichen, die Funktionalitäten nutzt oder auf Daten zugreift. Zugriffe auf geheime Informationen sind, sofern technisch möglich, zu protokollieren.

3.3.4 Risikomanagement

Die Durchführung von Risikobewertungen stellt ein zentrales Element der Informationssicherheit dar. Die Implementierung und Durchsetzung von Informationssicherheitsmaßnahmen müssen das mit der Nutzung von Informationen und IT-Systemen verbundene Risiko auf ein für GUD akzeptables Restrisiko reduzieren. Die getroffenen Maßnahmen müssen sich innerhalb eines akzeptablen Kostenrahmens bewegen sowie die Verantwortung und das Verhalten des Benutzers angemessen berücksichtigen.

3.3.5 Eigentümerschaft

Jedes System und jede Information hat einen Eigentümer, der festgelegte Pflichten zum Schutz der Systeme und Informationen hat. Dazu gehört die Festlegung der Anforderungen an die Integrität und Verfügbarkeit des Systems sowie die Vertraulichkeit.

4. Informationssicherheitsmanagementsystem (ISMS)

Zur Erreichung der vorgenannten Schutzziele hat die GUD-Geschäftsführung beschlossen, ein Informationssicherheitsmanagementsystem (ISMS) entsprechend den Anforderungen der internationalen Normen zur Informationssicherheit ISO 27001 sowie ISO 27019 in Verbindung mit den Vorgaben des IT-Sicherheitskatalogs der Bundesnetzagentur einzuführen, aufrecht zu erhalten und ständig zu verbessern.

4.1 Grundsätzliche Gestaltung des ISMS

Das GUD ISMS ist integraler Bestandteil des Gasunie Deutschland Managementsystems (GMS). Die im Rahmen des GMS definierten allgemein gültigen unternehmensweiten Prozesse und Regelungen finden auch für das ISMS Anwendung. Dieses gilt auch für die Vorgaben zur Erstellung, Revision, Ablage und Nutzung von Dokumenten.

Die vorliegende Informationssicherheitsrichtlinie bildet dabei die Grundlage für alle Informationssicherheitsanweisungen bei GUD. Basierend auf dieser Anweisung sind die Verantwortlichkeiten, organisatorische Maßnahmen sowie grundlegende Verfahren und Prinzipien der Informationssicherheit weiter definiert.

4.2 Stetige Verbesserung der Informationssicherheit

Die Geschäftsführung unterstützt die ständige Verbesserung des Sicherheitsniveaus und stellt dazu angemessene Ressourcen zur Verfügung. Alle Mitarbeitenden sind angehalten, mögliche Verbesserungen oder Schwachstellen an die hierfür jeweils benannten Stellen weiterzugeben. Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung soll das angestrebte Sicherheits- und Schutzniveau sichergestellt werden. Abweichungen werden mit dem Ziel analysiert, die Sicherheitssituation zu verbessern und ständig auf dem aktuellen Stand zu halten.

5. Anlagen

Keine