Leitlinie zur Informationssicherheit der GKS-Gemeinschaftskraftwerk Schweinfurt GmbH

1. Kontext

1.1 Einleitung
Die GKS-Gemeinschaftskraftwerk Schweinfurt GmbH (GKS) hat ein Managementsystem für Informationssicherheit (ISMS) im Rahmen des für GKS gültigen Managementsystem „High Level Structure“ etabliert, das den Anforderungen der ISO/IEC 27001 entspricht. Zentraler Bestandteil eines ISMS ist unter anderem die Leitlinie zur Informationssicherheit. Das vorliegende Dokument ist die Leitlinie zur Informationssicherheit der GKS.

1.2 Geltungsbereich
Der Geltungsbereich dieser Leitlinie entspricht dem Geltungsbereich des ISMS-Konzeptes des GKS. Diese Richtlinie gilt für alle Mitarbeitenden im Geltungsbereich.

1.3 Ansprechpartner
Der Ansprechpartner zu allen Fragen dieser Richtlinie ist der Informationssicherheitsbeauftragte (ISB) von GKS.

1.4 Verantwortlichkeiten
Die Gesamtverantwortung für die ordnungsgemäße Organisation und Überwachung der Informationssicherheit verbleibt bei der Geschäftsführung.

Die operative Verantwortung für die Sicherheit der IT- und OT-Systeme sowie die Umsetzung geeigneter technischer und organisatorischer Maßnahmen liegt bei der Technischen Leitung.

Der Informationssicherheitsbeauftragte (ISB) berät die Geschäftsführung und die Fachbereiche fachlich unabhängig und überwacht die Weiterentwicklung des ISMS.

Die organisatorische Umsetzung der Vorgaben erfolgt durch die jeweils zuständigen Führungskräfte in ihren Verantwortungsbereichen.

2. Stellenwert der Informationstechnologie und Informationssicherheit
Unternehmenszweck des GKS ist im Unternehmenshandbuch (UHB) dargestellt.
Informationssicherheit stellt für die GKS ein äußerst wichtiges Qualitätsmerkmal der Datenverarbeitung dar, da alle wesentlichen strategischen und operativen Geschäftsprozesse im Unternehmen durch Informationstechnologie (IT) maßgeblich unterstützt werden.

Ziel des Unternehmens ist es, die Daten und IT-Systeme (BT (Büro-IT) und OT (Leittechnik)) in allen technikabhängigen und kaufmännischen Bereichen in ihrer Verfügbarkeit so zu sichern, dass die zu erwartenden Stillstandzeiten und der maximale Datenverlust toleriert werden können. Für den Anlagenbetrieb besitzt die Verfügbarkeit der OT-Systeme eine besondere Priorität. Auch gilt es, die Integrität und Vertraulichkeit von sensiblen Unternehmensdaten und personenbezogenen Daten in ausreichender Weise zu sichern.

Beeinträchtigungen hinsichtlich der Verfügbarkeit der unternehmenseigenen Applikationen können ebenso gravierende Auswirkungen nach sich ziehen wie Unregelmäßigkeiten in Bezug auf die Integrität und Vertraulichkeit der verarbeiteten bzw. benutzten Informationen.

3. Unternehmensziele hinsichtlich Informationssicherheit

Die Geschäftsführung der GKS-Gemeinschaftskraftwerk GmbH hat auf Grund des Stellenwertes der Informationssicherheit für die Geschäftsziele entschieden, dass ein angemessenes Sicherheitsniveau angestrebt werden soll.

Grundlage für diese Entscheidung waren die Werte der zu schützenden Güter sowie des vertretbaren Aufwands an Personal und Finanzmitteln für Informationssicherheit. Risiken, die zu längeren Produktionsausfällen oder erheblichen Beeinträchtigungen des Anlagenbetriebs führen können, werden nicht akzeptiert. Dies bedeutet im Einzelnen:

3.1 Bewusstsein für Informationssicherheit

Um Informationssicherheit gewährleisten zu können, sind angemessene technische und organisatorische Maßnahmen erforderlich. Diese können nur dann hinreichend wirksam sein, wenn alle Beschäftigten die möglichen Gefährdungen für die Informationssicherheit kennen und in ihren Aufgabenbereichen entsprechend verantwortlich handeln. Regelmäßige Fortbildungen zur Informationssicherheit können hierbei unterstützen.

3.2 Einhaltung von Gesetzen oder Vorschriften

Die Maßnahmen für Informationssicherheit sollen auch dazu beitragen, dass die für das Unternehmen relevanten Gesetze, Vorschriften und vertragliche Verpflichtungen eingehalten werden. Wichtigste Gesetze, Vorschriften und vertragliche Verpflichtungen sind im Rechtskataster der GKS dokumentiert.

3.3 Funktionale Aufgabenerledigung

Die Informationstechnik muss so betrieben werden, dass Geschäftsinformationen hinreichend schnell verfügbar sind. Ausfälle, die zu Terminüberschreitungen führen sind nicht tolerierbar. Die Informationssicherheit unterstützt damit auch eine funktionale Aufgabenerledigung.

3.4 Vermeidung materieller und Umwelt-Schäden

Unmittelbare oder mittelbare finanzielle Schäden können durch den Verlust der Vertraulichkeit schutzbedürftiger Daten, die Veränderung von Daten oder den Ausfall einer IT-Anwendung oder eines Systems entstehen. Dies Vermeidung materieller und immaterieller Schaden muss als hoch angesiedeltes Ziel stehen. Informationssicherheit wirkt damit auch u.a. materiellen Schäden entgegen.

3.5 Wahrung von Persönlichkeitsrechten und Betriebsgeheimnissen

Vertraulichkeit und Integrität der für das Unternehmen wichtigen Informationen sind zu schützen, unabhängig davon, in welcher Form sie vorliegen

3.6 Vermeidung von Ansehensverlust bzw. Imageschaden, Sozial-Schäden

Finanzielle Schäden und ein negatives Image für das Unternehmen müssen verhindert werden. Informationssicherheit vermeidet damit Ansehensverlust und Imageschaden sowie Verlust sozialer Akzeptanz des Unternehmens.

3.7 Kontinuierliche Verbesserung

Und ferner strebt die GKS-Gemeinschaftskraftwerk GmbH die kontinuierliche Verbesserung seiner Prozesse rund um die Informationssicherheit an. Sicherheitsvorfälle sind systematisch zu erfassen, zu analysieren und zur Verbesserung des ISMS zu nutzen.

4. Organisation des Managementsystems für Informationssicherheit

Grundsätzlich wird im Unternehmenshandbuch von GKS in Kapitel 3.1 die Aufbauorganisation beschrieben. Die wesentlichen Rollen hinsichtlich der Informationssicherheit und deren Verantwortlichkeiten innerhalb des ISMS der GKS-Gemeinschaftskraftwerk GmbH sind zum besseren Verständnis hier dargestellt:

4.1 Geschäftsführung

Die Geschäftsführung ist das oberste Entscheidungsgremium. Sie verabschiedet auf Vorschlag des Informationssicherheitsbeauftragten diese Informationssicherheitsleitlinie.
Die Geschäftsführung ist dafür verantwortlich, sicherzustellen, dass das ISMS entsprechend dieser Richtlinie umgesetzt und aktualisiert wird und dass die notwendigen Ressourcen verfügbar sind. Der Technischen-Leitung und dem Informationssicherheitsbeauftragten werden von der Geschäftsführung ausreichende finanzielle und zeitliche Ressourcen zur Verfügung gestellt, um sich regelmäßig weiterzubilden, zu informieren und die vom Management festgelegten Sicherheitsziele zu erreichen.
Die Geschäftsleitung muss das ISMS mindestens einmal jährlich überprüfen (bzw. immer im Falle von erheblichen Änderungen) und freigeben. Zweck dieser Überprüfung durch das Management ist der Nachweis der Angemessenheit, Eignung und Wirksamkeit des ISMS (siehe Bestellungen).Die Gesamtverantwortung für die ordnungsgemäße und sichere Aufgabenerfüllung (und damit die Informationssicherheit) verbleibt bei der Unternehmensleitung.

4.2 Technische Leitung

Die zentrale Instanz für die operative Sicherheit der Informationstechnik (IT) ist die Technische Leitung (TL). Sie ist für den sicheren Betrieb und damit die Umsetzung geeigneter Sicherheitsmechanismen verantwortlich.
In Zusammenarbeit mit dem Informationssicherheitsbeauftragten bringt sie die für die Informationssicherheit spezifischen Aspekte und Anliegen ein und ist für die Umsetzung geeigneter Sicherheitsmaßnahmen zuständig.
Die TL stellt sicher, dass der Informationssicherheitsbeauftragte frühzeitig in alle IT-Projekte eingebunden wird.

4.3 Informationssicherheitsbeauftragter (ISB)

Der Informationssicherheitsbeauftragte ist für die Koordination des Betriebs des ISMS verantwortlich sowie für die Berichterstattung über dessen Leistungsfähigkeit. Der Informationssicherheitsbeauftragte übt seine Aufgaben fachlich unabhängig aus.
Er ist des Weiteren für die Koordination bzw. Umsetzung von Informationssicherheitstrainings und -programmen zur Bewusstseinsbildung (Awareness) für Mitarbeitende verantwortlich. Er ist für die Aufstellung und Implementierung des Plans für Training und Awareness verantwortlich, dem alle Personen unterliegen, die eine Rolle im ISMS innehaben.
Der Informationssicherheitsbeauftragte definiert, welche sich auf Informationssicherheit beziehenden Informationen durch wen und wann kommuniziert werden. Dies gilt sowohl für interne als auch externe Parteien.
Die Einführung neuer Anwendungen, Verfahren, Prozesse und Infrastrukturkomponenten bedarf einer Freigabe durch den Informationssicherheitsbeauftragten. Dabei muss besonderes Augenmerk darauf gerichtet werden, dass durch den Einsatz der neuen Komponenten und Verfahren keine unverhältnismäßigen Risiken hinsichtlich Informationssicherheit entstehen oder Risiken erhöht werden.
Der Informationssicherheitsbeauftragte berät die Geschäftsführung und die Fachbereiche in Fragen der Informationssicherheit und arbeitet mit der IT-Leitung zusammen. Er beobachtet laufend die technischen und organisatorischen Fortentwicklungen im Bereich der Informationssicherheit und schlägt in
Abstimmung mit der Technischen-Leitung die notwendigen Maßnahmen vor. Des Weiteren ist er frühzeitig in alle Projekte einzubinden, um schon in der Planungsphase alle sicherheitsrelevanten Aspekte berücksichtigen zu können.

4.4 Informationssicherheits-Management-Team (ISMS-Team)

Das ISMS-Team setzt sich aus dem Informationssicherheitsbeauftragten, der Technischen Leitung sowie fachkundigen Mitarbeitern für die Administration und für den Betrieb zusammen. Das ISMS-Team hält regelmäßige Treffen ab.

Das ISMS -Team plant die notwendigen Tätigkeiten zur Aufrechterhaltung und Verbesserung der Informationssicherheit. Weiterhin werden im ISMS-Management-Team Audits geplant und Sicherheitsvorfälle besprochen. Im ISMS -Team werden auch die Dokumente des ISMS laufend überprüft und überarbeitet. Planungen und Änderungen im Anwendungsbereich sind stets im ISMS-Team abzustimmen.

4.5 Mitarbeiter

Die Mitarbeiter sollen sich stets der Bedeutung der Informationssicherheit bewusst sein und aktiv an der Abwehr und Bekämpfung von materiellen und ideellen Schäden mitwirken. Sie sollen verantwortungsbewusst mit den Informationssystemen und den darauf gespeicherten und dort verarbeiteten Daten umgehen und auf die Wahrung von Betriebs- und Geschäftsgeheimnissen achten.
Der Schutz der Integrität, Verfügbarkeit und Vertraulichkeit von Werten unterliegt der Verantwortung der Eigentümer der jeweiligen Werte. Bei Unregelmäßigkeiten müssen die Mitarbeiter unverzüglich den Informationssicherheitsbeauftragten und ihre Vorgesetzten informieren. Es wird erwartet, dass jeder Nutzer von IT-Systemen die vorliegende Informationssicherheitsleitlinie kennt und beachtet.

4.6 Weitere Verantwortlichkeiten

Für alle Informationen, Geschäftsprozesse sowie die unterstützenden informationstechnischen Systeme und Infrastruktureinrichtungen werden Verantwortliche (Informations-, Prozess- und Systemeigentümer Eigentümer von Zielobjekten) benannt. Diese sind dafür zuständig, die geschäftliche Bedeutung von Informationen und Technik einzuschätzen und darauf zu achten, dass die Mitarbeiter dieser Bedeutung entsprechend handeln. Sie verwalten Zugriffsrechte und Autorisierungen in ihrem Zuständigkeitsbereich und sind gegenüber der Leitung rechenschaftspflichtig. Sie sind auch dafür verantwortlich, externen Dienstleistern und Kooperationspartnern die Vorgaben der GKS zur Informationssicherheit zur Kenntnis zu geben und deren Einhaltung zu überwachen.

5. Folgen von Zuwiderhandlungen

Beabsichtigte oder grob fahrlässige Handlungen, die Sicherheitsvorgaben verletzen, können finanzielle Verluste bedeuten, Mitarbeiter, Geschäftspartner und Kunden schädigen oder den Ruf des Unternehmens gefährden. Bewusste Verstöße gegen verpflichtende Sicherheitsregeln können arbeitsrechtliche und unter Umständen auch strafrechtliche Konsequenzen haben und zu Regressforderungen führen.

6. Weitere Maßnahmen

Ausgehend von den Anforderungen der Norm ISO/IEC 27001 zur Einführung und Aufrechterhaltung eines Managementsystems für Informationssicherheit wurden diverse weiterführende Regelungen geschaffen, die dieses ISMS konkretisieren und gleichfalls gültig sind.

7. Inkraftsetzung

Dieses Dokument wird einmal jährlich sowie bei Bedarf auf Vollständigkeit und Aktualität überprüft.

Schweinfurt, den 23.02.2026

Dr.-Ing. Ingo Zorbach