


<b>MANAGEMENTHANDBUCH</b>  <b>MHKW KASSEL</b>	 Müllheizkraftwerk Kassel GmbH
<b>Informationssicherheitspolitik</b>	Rev.-Index: 1 Datum: 12.11.2025 Seite: 1 von 6

	erstellt	geprüft	freigegeben	freigegeben
Org.-Einheit	ISB	EM	GF	GF
Name	Timm Vollmer (extern)	Heiko Dreger	Dr. Gudrun Stieglitz	Dr. Mark Eppe
Datum	12.11.2025	11.02.2026	03.03.2026	03.03.2026
Unterschrift	Gez. Vollmer	Gez. Dreger	Gez. Stieglitz	Gez. Eppe
Sicherheitsklassifikation	<b>Öffentlich</b> <input checked="" type="checkbox"/>	<b>Intern</b> <input type="checkbox"/>	<b>Vertraulich</b> <input type="checkbox"/>	

## Inhaltsverzeichnis

1	Einleitung.....	3
2	Grundsätze .....	4
3	Informationsschutzziele.....	5
4	Leitgedanken und Umsetzung.....	6
5	Unsere Verantwortlichkeiten .....	6

## 1 Einleitung

Die MHKW Kassel GmbH ist bereits seit mehr als 50 Jahren ein wichtiger Dreh- und Angelpunkt für die Produktion von Strom und Wärme sowie der Abfallentsorgung in der Region. Der Schutz unserer Informationen und Werte ist daher unverzichtbar.

Diese Informationssicherheitspolitik definiert die verbindlichen Grundsätze, Ziele und organisatorischen Rahmenbedingungen. Zum Schutz von Informationen, Systemen und Diensten des Müllheizkraftwerks (MHKW). Sie dient der Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Belastbarkeit aller Informationsverarbeitungsprozesse und technischen Anlagen.

Sie etabliert das strategische Fundament für unser Informationssicherheitsmanagementsystem gemäß ISO/IEC 27001:2022.

Das MHKW erfüllt alle gesetzlichen Verpflichtungen als KRITIS-Betreiber. Dies gewährleistet höchste Sicherheitsstandards für unsere kritische Infrastruktur im Sektor Siedlungsabfallentsorgung.

Die Geschäftsführung bekennt sich zur Informationssicherheit und trägt die Gesamtverantwortung für die Informationssicherheit, stellt angemessene Ressourcen bereit und verankert die Ziele verbindlich in Strategie, Planung und Betrieb.

Dies dient als Grundlage für den sicheren Betrieb des Müllheizkraftwerks mit dem Zweck der Verwertung von Hausmüll. Bei der Abfallverwertung wird auch Strom und Fernwärme erzeugt.

Diese Politik richtet sich an alle Mitarbeiter, Führungskräfte, Auftragnehmer, Dienstleister, Lieferanten und weitere Stakeholder, die direkt oder indirekt mit unseren Informationsverarbeitungssystemen interagieren oder Einfluss auf unsere Informationssicherheit haben.

Der Schutz unserer Informationen und Werte hat einen maßgeblich hohen Stellenwert für uns. Zusätzlich ist es in unserer Position für Kassel und der Region unabdingbar, dass wir uns kontinuierlich verbessern, dass wir uns den stetig ändernden Anforderungen und Bedrohungen der Technologie anpassen sowie neue gesetzliche Vorgaben umsetzen und einhalten.

Die MHKW GmbH sieht sich als Verpflichtung für die Zukunft in diesem Bereich weiter beispielhaft voranzugehen. Deshalb haben wir in unserem Unternehmen ein Informationssicherheitsmanagementsystem (ISMS) implementiert, welches diese Aspekte vereinigt und umsetzt.

Um diese Umsetzung zu ermöglichen, halten wir uns an unsere Richtlinien zur Informationssicherheit. Es sind klare Verantwortlichkeiten definiert und ausreichende Ressourcen zur Verwirklichung bereitgestellt.

Jedem Mitarbeiter ist die Wichtigkeit seines Mitwirkens zur Verbesserung an unserem ISMS bewusst und dass sie sich bei Fragen und Anregungen jederzeit an unseren Informationssicherheitsbeauftragten (ISB) wenden dürfen. Die Mitarbeiter werden zusätzlich regelmäßig geschult, sei es durch spezifischen Pflichtschulungen oder Veröffentlichungen im Intranet.

Unser ISB ist nicht nur für die Planung, Umsetzung, Überwachung und Verbesserung unseres ISMS zuständig oder als Ansprechpartner für unsere Mitarbeiter erreichbar. Er steht zudem auch Kunden, Lieferanten, Behörden und weiteren interessierten Parteien für Informationen gerne zur Verfügung. Einschließlich der Geschäftsleitung wird der Grundsatz der Informationssicherheit und das kontinuierliche Verbessern unserer Prozesse und Systeme von jedem in unserem Unternehmen gelebt.

## 2 Grundsätze

Das ISMS unterläuft einen ständigen Kreislauf der Verbesserung, der auch als PDCA-Zyklus bekannt ist. Unser Unternehmensgrundsatz beruht darauf, dass man niemals ausgelernt hat und sich ständig weiterentwickelt. Deshalb ist uns der PDCA-Zyklus besonders wichtig. Wir wenden ihn wie folgt an:

**Plan.** Wir legen Ziele, Prozesse, Regelungen oder Verfahren fest.

**Do.** Die festgelegten Ziele, Prozesse, Regelungen oder Verfahren werden entsprechend unserer Vorgaben unseres ISMS umgesetzt und Maßnahmen implementiert.

**Check.** Die Effektivität und Effizienz der Maßnahmen werden anhand der praktischen Erfahrung, durch interne Audits oder Managementbewertungen geprüft. Handlungs- und Optimierungsbedarf wird in diesem Schritt festgestellt.

**Act.** Anhand der Ergebnisse aus der Check-Phase werden Korrektur- und Präventionsmaßnahmen ergriffen und umgesetzt.

Um die erfolgreiche Umsetzung zu Prüfen und zu messen, beginnen wir wieder bei der Plan-Phase und der Kreislauf beginnt von vorn.

Potenzielle Sicherheitsvorfälle werden hierdurch mit angemessenen Gegenmaßnahmen auf allen Ebenen verhindert. Dies umfasst neben der Umsetzung von Schutzmaßnahmen zur Sicherstellung des ordnungsgemäßen Betriebs der Informationstechnik auch den Schutz von nicht elektronisch verarbeiteten Informationen durch entsprechende Sicherheitsprozesse. Die erfolgreiche Umsetzung der Sicherheitsprozesse ist nur mit der kooperativen Unterstützung aller Mitarbeiter, Partnern und sonstigen Dritten möglich.

## 3 Informationsschutzziele

Grundlegend ist es unser Ziel die Verfügbarkeit, Vertraulichkeit und die Integrität von Informationen sicherzustellen. Das verstehen wir darunter:

### Verfügbarkeit

Informationen, Anwendungen, IT / OT-Systeme und die Leittechnik stehen für Berechtigte im vorgesehenen Umfang sowie in angemessener Zeit zur Verfügung. Um dies zu erreichen, schützen wir unsere Daten und Informationen mithilfe von angemessenen Schutzmaßnahmen und Datensicherungen.

### Vertraulichkeit

Schützenswerte Informationen sind ausschließlich berechtigten Nutzern zugänglich. Dies ermöglichen wir durch Verschlüsselung von Daten und einer definierten Verteilung von Berechtigungen.

### Integrität

Schützenswerte Informationen bleiben unversehrt und vollständig. Damit wir dies gewährleisten können, vereinen wir Aspekte aus der Verfügbarkeit und Vertraulichkeit und ergänzen dies mit einer nachvollziehbaren Dokumentation und Versionskontrollen.

Die übergeordneten Ziele des ISMS sind:

- Schutz sensibler und geschäftskritischer Daten vor Verlust, Missbrauch oder unberechtigtem Zugriff,
- Sicherstellung der Einhaltung gesetzlicher, regulatorischer und vertraglicher Verpflichtungen,
- Minimierung der Risiken für Geschäftsprozesse durch angemessene technische und organisatorische Maßnahmen,
- Förderung des Sicherheitsbewusstseins aller Mitarbeiterinnen und Mitarbeiter,
- Etablierung eines Prozesses zur kontinuierlichen Verbesserung der Informationssicherheit.

Konkrete **messbare Informationssicherheitsziele** werden jährlich festgelegt, überprüft und im Rahmen des Management-Reviews bewertet.

## 4 Leitgedanken und Umsetzung

Unser Leitgedanke ist ein gelebtes ISMS, Freude an der Informationssicherheit und die Unterstützung unserer Mitarbeiter ohne Zurückhaltung. Verbunden mit unserem Fachwissen und unserer Erfahrung kann jeder auf einen sorgfältigen Umgang mit Daten und Informationen vertrauen.

Wir zeichnen uns durch eine ausgeprägte interne Kommunikation, eine angemessene Verteilung von Berichtungen sowie ein starkes Bewusstsein über die Informationssicherheit bei allen Beteiligten im Unternehmen aus.

Um diese Leitgedanken erfolgreich umzusetzen, gehen wir wie folgt vor:

In unserer Berechtigungs- und Zutrittsverwaltung wird der Zugriff und Zugang zu Daten, Informationen, Systemen sowie des Gebäudes und zu Räumen klar definiert und nur nach dem entsprechenden Bedarf zur Verfügung gestellt.

Schutz von Informationen und der Umgang mit vertraulichen Inhalten auf Dokumenten und Datenträgern ist ein elementarer Aspekt unseres ISMS. Wir verzichten zum Großteil auf das Ausdrucken von sensiblen Daten und stellen eine sicherere Aufbewahrung von Dokumenten und Datenträgern in verschlossenen und vorgesehenen Bereichen sicher. Die ordnungsgemäße Entsorgung von Dokumenten und Datenträgern liegen in der Verantwortung eines jeden Mitarbeiters in unserem Unternehmen.

Die Aktualität und Angemessenheit der technischen Sicherheit und Anforderungen in unserem Unternehmen sind ein weiterer wichtiger Bestandteil sowie ein Aushängeschild unseres Unternehmens.

Bei jedem unserer Mitarbeiter stellen wir ein grundlegendes Bewusstsein über die Informationssicherheit sicher. Deshalb ist jeder Mitarbeiter eigenverantwortlich dazu angehalten, die Sicherstellung der Informationssicherheit zu unterstützen und Schwachstellen, Situationen und Vorfälle zu melden. Um dieses Bewusstsein zu schaffen, führen wir regelmäßig Schulungen durch.

## 5 Unsere Verantwortlichkeiten

- Die **Geschäftsführung** trägt die Gesamtverantwortung für die Informationssicherheit sowie die Einhaltung aller rechtlichen Vorgaben und stellt die erforderlichen Ressourcen bereit.
- Der **Informationssicherheitsbeauftragte (ISB)** ist für die Umsetzung, Überwachung und kontinuierliche Verbesserung des ISMS verantwortlich.
- Alle **Mitarbeiterinnen und Mitarbeiter** sind verpflichtet, diese Politik und alle relevanten Sicherheitsrichtlinien einzuhalten und Sicherheitsvorfälle unverzüglich zu melden.
- **Externe Dienstleister** werden vertraglich zur Einhaltung der Informationssicherheitsanforderungen verpflichtet.