



Informationssicherheitsrichtlinie

Dokumententitel	Information Security Policy - Public
Dokumenten-ID	MM-ISMS-PL-01
Eigentümer	Marcel Lehner (CISO)
Genehmiger	Peter Oswald (CEO), Franz Hiesinger (CFO), Jacqueline Wild (Head of Group IM)
Kontakt	Group Security security@mm.group
Wirksamkeitsdatum	01.02.2018
Letzte Aktualisierung	01.07.2022

1 Leitbild

Die Mayr-Melnhof Karton AG / MM Group (MM) ist der weltweit führende Hersteller von beschichtetem Recycling-Karton und der größte Anbieter von Faltschachteln in Europa. Unser Ziel ist es, durch innovative und umweltfreundliche Verpackungs- und Papierlösungen Nachhaltigkeit zu fördern. Wir setzen dabei auf modernste Informations- und Kommunikationstechnologien und -prozesse.

Wir sind uns der kritischen Bedeutung der sicheren und zuverlässigen Informationsverarbeitung bewusst und haben deshalb bei MM ein starkes Engagement für Informationssicherheit. Technische Störungen, Fehlverhalten, Sabotage und Spionage können die Funktionalität und Verfügbarkeit unserer IT-Systeme und -Netzwerke sowie die Vertraulichkeit und Integrität unserer Geschäftsprozesse und -daten erheblich gefährden. Im schlimmsten Fall könnte dies unseren Ruf schädigen, finanzielle Verluste verursachen und potenzielle Risiken für Mensch und Umwelt verursachen.

Um diese Risiken zu minimieren, haben wir ein integriertes Informationssicherheitsmanagementsystem (ISMS) nach international anerkannten Standards eingeführt, das Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität nachhaltig und kosteneffektiv gewährleistet.

1.1 Informationssicherheitskultur

Wir bei MM schätzen das Vertrauen unserer Kunden in unsere Dienstleistungen, insbesondere wenn es um die Qualität und Sicherheit ihrer Daten und Informationen geht. Wir wissen, dass diese für den reibungslosen Betrieb unserer Produktionsstätten und unseres Geschäfts sowie für die Verarbeitung kundengenerierter Daten unerlässlich sind.

Deshalb ergreifen wir alle notwendigen und wirtschaftlich vertretbaren Maßnahmen, um die Sicherheit und den Schutz unserer Dienstleistungen, Einrichtungen, Daten und Informationen zu gewährleisten. Wir verwenden die neuesten Technologien und halten uns an die höchsten Standards, um sicherzustellen, dass die Integrität, Verfügbarkeit und Vertraulichkeit unserer Daten und Informationen jederzeit gewährleistet sind.

Unser Engagement für Informationssicherheit ist ein zentraler Bestandteil unserer Unternehmenskultur bei MM. Es ist fest in unseren informellen Strukturen verankert und wird durch das Handeln unseres Managementteams verkörpert. Wir sind bestrebt, diese Kultur in allen unseren Mitarbeitern zu fördern und sicherzustellen, dass Informationssicherheit für jeden bei MM oberste Priorität hat.



1.2 Ziele der Informationssicherheit

Bei MM priorisieren wir die Informationssicherheit. Unsere Ziele umfassen:

- Laufende Verbesserung und Aktualisierung unserer Sicherheitsmaßnahmen, um uns an die sich ständig verändernde Bedrohungslage anzupassen und sicherzustellen, dass wir potenziellen Risiken und Schwachstellen immer einen Schritt voraus sind.
- Einhaltung gesetzlicher Anforderungen für Informationssicherheit und Datenschutz in angemessener und umfassender Weise.
- Anwendung von modernsten Methoden zur Sicherung unserer Dienstleistungen, Einrichtungen, Daten und Informationen, um unbefugten Zugriff oder Diebstahl zu verhindern.
- Evaluierung der Risiken neuer Technologien und Integration der Informationssicherheit in unsere Entscheidungsprozesse für Beschaffung und Betrieb, unter Berücksichtigung von Effizienz und Benutzerfreundlichkeit.
- Bereitstellung regelmäßiger Schulungs- und Sensibilisierungsprogramme für unsere Mitarbeiter, um ein Bewusstsein für Informationssicherheit zu schaffen und sie in die Lage zu versetzen, potenzielle Sicherheitsvorfälle zu erkennen und zu verhindern.
- Etablierung eines transparenten und effizienten Incident-Response-Plans zur schnellen Identifizierung, Eindämmung und Behebung von Sicherheitsverletzungen, um deren Auswirkungen zu minimieren und zukünftige Vorfälle zu verhindern.

1.3 Informationssicherheitsstrategie

Unsere Ziele wurden durch die Umsetzung der folgenden Punkte erreicht:

- Es wurde ein Informationssicherheitsmanagementsystem (ISMS) auf Basis international anerkannter Standards eingerichtet.
- Ein Informationssicherheitsrisikomanagementsystem (IS-RM) wurde implementiert, um das Management mit den erforderlichen Informationen für fundierte Entscheidungen bezüglich der Informationssicherheitsrisiken zu versorgen.
- Ein Schulungs- und Sensibilisierungsprogramm wurde von unserem Team etabliert, um sicherzustellen, dass alle Mitarbeiter auf dem neuesten Stand der technischen Kenntnisse und Best Practices im Bereich Informationssicherheit sind.
- Key Performance Indicators (KPIs) und Audit-Maßnahmen wurden etabliert, um kontinuierlich die Effektivität und Qualität unseres ISMS und unserer operativen Maßnahmen zu bewerten und zu verbessern.
- Wir haben Prozesse für die gesetzlich vorgeschriebene Kommunikation mit Behörden und Kunden im Falle von Sicherheitsvorfällen oder Anfragen im Zusammenhang mit personenbezogenen Daten und Informationen implementiert.

2 Geltungsbereich

Unsere Informationssicherheitsrichtlinie gilt für MM und alle seine Tochtergesellschaften weltweit und deckt alle Aspekte unseres Geschäftsbetriebs ab, einschließlich Prozesse, Vermögenswerte und Informationen, die für die Erreichung unserer Unternehmensziele von entscheidender Bedeutung sind. Wir erwarten von allen Auftragnehmern, dass sie diese Richtlinie verstehen und befolgen, insbesondere beim Kauf neuer IT-Systeme. Wir stellen sicher, dass diese Anforderungen in unseren Einkaufsbedingungen und Planungsdokumenten enthalten sind und beziehen uns ebenfalls bei der Erstellung individueller Verträge darauf. Wir erwarten auch von allen Mitarbeitern, dass sie die unten aufgeführten Grundsätze und Standards einhalten.



3 Grundsätze

Mayr-Melnhof Karton AG / MM Group (MM) hat ein umfassendes Informationssicherheitsmanagementsystem (ISMS) implementiert, das nach international anerkannten Standards und Frameworks wie ISO/IEC 27001:2022 ausgerichtet ist und kontinuierlich verbessert wird. Dieses System basiert auf folgenden Grundsätzen

- Unsere Informationssicherheitsziele sind auf MM's Gesamtziele abgestimmt und fördern eine Kultur der Sicherheitsbewusstheit und des Sicherheits-Engagements im gesamten Unternehmen.
- Informationssicherheitsmaßnahmen und Risikomanagementprozesse leiten sich aus unserer Informationssicherheitsrichtlinie ab. Wir verwenden grundlegende Schutzmaßnahmen und detaillierte Risikoanalysen, um ein risikoadaptives Sicherheitsniveau zu erreichen.
- Unsere Auswahl und Implementierung von Informationssicherheitsmaßnahmen erfolgt auf der Grundlage des Risikoniveaus unter Berücksichtigung des Standes der Technik. Wir überprüfen und aktualisieren diese Maßnahmen regelmäßig im Rahmen unseres kontinuierlichen Verbesserungsprozesses.
- Mitarbeiter erhalten nur die für ihre Aufgaben erforderlichen Informationen, wobei technische und organisatorische Maßnahmen einen Informationsüberfluss verhindern. Wir trennen inkompatible Funktionen, Rollen und Verantwortlichkeiten, um Fehler und Manipulationen zu vermeiden. Wenn eine funktionale Trennung nicht möglich ist, implementieren wir kompensierende Maßnahmen.
- Wir führen Protokolle aller Informationen, die aufgrund der Informationssicherheitsrichtlinie zugänglich sind, und stellen sicher, dass der Zugriff ausschließlich im Rahmen zugewiesener Aufgaben erfolgt.
- Interne und externe Audits sowie regelmäßige Risikoanalysen bewerten die Einhaltung der Grundsätze und die Wirksamkeit unseres Informationssicherheitsmanagementsystems. Wir dokumentieren die Ergebnisse und leiten daraus Verbesserungsmaßnahmen ab.
- Daten und Informationen werden basierend auf Vertraulichkeit, Integrität, Verfügbarkeit und Datenschutzrelevanz klassifiziert. Wir bieten unseren Mitarbeitern regelmäßig Schulungen und Sensibilisierungsinitiativen an, um verantwortungsbewusste Informationsverarbeitung zu fördern.
- Wir wenden die Anforderungen des Informationssicherheitsmanagementsystems (ISMS) auf neue IT-Systeme an. Für bestehende Systeme haben wir einen Übertragungsprozess etabliert.
- Wir unterhalten ein angemessenes Leistungsmesssystem, um unser Informationssicherheitsmanagementsystem kontinuierlich zu verbessern.
- Incident-Management-Prozesse sind implementiert, um Sicherheitsvorfälle zu identifizieren, zu bewerten und zu reagieren, wobei eine zeitnahe Kommunikation und Lösung sichergestellt wird.
- Drittanbieter und Partner werden sorgfältig bewertet, um sicherzustellen, dass sie unseren Informationssicherheitsstandards entsprechen und Datenschutzanforderungen einhalten.
- Business-Continuity- und Notfallwiederherstellungspläne werden regelmäßig erstellt, getestet und aktualisiert, um potenzielle Störungen zu minimieren und eine schnelle Wiederherstellung der Betriebsfähigkeit sicherzustellen.
- Die kontinuierliche Überwachung und Verbesserung unseres Informationssicherheitsmanagementsystems erfolgt durch die Erfassung und Analyse relevanter Kennzahlen, die Entscheidungsfindung unterstützen und uns dabei helfen, Bereiche zur Verbesserung zu identifizieren

4 Durchsetzung und Sanktionierung

Unser Managementteam ist verantwortlich, dafür zu sorgen, dass angemessene Informationssicherheitsmaßnahmen umgesetzt werden. Wir überwachen aktiv die Einhaltung dieser Sicherheitsmaßnahmen. Wenn Mitarbeiter oder Partner ihnen nicht folgen, wird unser Managementteam sie über ihre Verantwortlichkeiten informieren. Bei Bedarf werden Verstöße angemessen geahndet.



5 Verbindlichkeitserklärung

MMs Managementteam hat eine Informationssicherheitsrichtlinie Version 2.0, gültig ab dem 1. Juli 2022, erlassen. Diese Richtlinie bildet die Grundlage für alle IT-bezogenen Entscheidungen und Maßnahmen innerhalb des Unternehmens. Sie stimmt mit unseren breiteren Unternehmensstrategien überein und ist entscheidend für die Erreichung unserer Geschäftsziele und die Umsetzung unserer IT-Strategie. MM ist bestrebt, diese Informationssicherheitsrichtlinie umzusetzen, aufrechtzuerhalten und kontinuierlich zu verbessern.

Ab dem 1. Juli 2022 sind die Informationssicherheitsrichtlinie, zugehörige Standards, Richtlinien und Arbeitsanweisungen für alle Mitarbeiter von MM, einschließlich derer in Mehrheitsbesitz befindlichen Tochtergesellschaften, verbindlich. Diese Richtlinie gilt auch für externe Dienstleistungspartner und Personal, das für MM und alle vom Group IM verwalteten Geschäfte tätig ist.



MMag. Peter Oswald
(CEO)



Mag. Franz Hiesinger
(CFO)



Jacqueline Wild
Head of Group IM