Informationssicherheitspolitik

Inhaltsverzeichnis

1. Leitbild

Die Mayr-Melnhof Karton AG (in der Folge „MM Gruppe“ bzw „MM“) ist der weltweit größte Hersteller von gestrichenem Recyclingkarton, sowie Europas führender Produzent von Faltschachteln. Die strategische Ausrichtung der MM Gruppe basiert auf vier Säulen: Konzentration auf Kernkompetenzen, Markt- und Kostenführerschaft, langfristige Ergebnisorientierung und Expansion.

Bei der Umsetzung dieser strategischen Zielsetzung stellen Geräte und Verfahren der Informations- und Kommunikationstechnologie einen bedeutenden Faktor dar. Diese Technologien sind notwendig, um sowohl die innerbetrieblichen Abläufe als auch Beschaffungsvorgänge und die Lieferungen und Leistungen für unsere Kunden zeitgerecht, kosteneffizient und mit der notwendigen Qualität zu erbringen. Zudem ist eine hohe Abhängigkeit von einer sicheren und stets verfügbaren Informationsverarbeitung gegeben. Die Funktionsfähigkeit und Verfügbarkeit der informationstechnischen Systeme und Netze sowie die Vertraulichkeit und Integrität der Geschäftsprozesse und Daten sind durch technische Fehler, Fehlverhalten, Sabotage und Spionage ständig gefährdet. Dies kann zu Imageverlust, wirtschaftlichem Schaden und im Extremfall zur Gefährdung von Umwelt und Menschen führen.

Vor diesem Hintergrund hat die Informationssicherheit in der MM Gruppe sehr hohen Stellenwert. Das Unternehmen betreibt daher ein integriertes Informationssicherheitsmanagementsystem (ISMS) welches die Aspekte Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität wirkungsvoll, nachhaltig und kostengünstig sicherstellt.

1.1. Informationssicherheitskultur

Das Vertrauen der Kunden in die Qualität und Sicherheit der Dienstleistungen ist der MM Gruppe ein sehr hohes Gut. Dies schließt sowohl Daten und Informationen ein, die zum sicheren Betrieb der Büroumgebung und der technischen Anlagen benötigt werden, als auch die Daten und Informationen, die beim Kunden generiert werden und personenbezogen verarbeitet werden. Zum Schutz ihrer Dienstleistungen, Anlagen, Daten und Informationen trifft die MM Gruppe alle notwendigen und wirtschaftlich vertretbaren Maßnahmen um diese Werte gemäß dem Stand der Technik zu schützen.

Diese Informationssicherheitskultur ist Bestandteil der Unternehmenskultur von MM und bestimmt die Wahrnehmung, das Denken und das Handeln in Bezug auf Informationssicherheit. Sie gehört damit zu den informellen Strukturen und wird durch ihre Leitungsorgane vorbildhaft gelebt, weiterentwickelt und den Mitarbeitern vermittelt.

1.2. Ziele der Informationssicherheit

Um die Anforderungen aus den Rahmenbedingungen und aus der Sicherheitskultur gerecht zu werden, definiert die MM Gruppe folgende Ziele zur Informationssicherheit:

- Es sollen Rahmenbedingungen geschaffen werden, Dienstleistungen, Anlagen, Daten und Informationen gemäß dem Stand der Technik gegen Manipulation oder Entwendung abzusichern.
- Es sollen Rahmenbedingungen geschaffen werden, die beim Einsatz neuer Technologien, die Informationssicherheit als einen gleichwertigen Bestandteil zu Wirtschaftlichkeit und Usability in eine risikobasierende Bewertung für Beschaffung und Betrieb einbringt.
- Es sollen Rahmenbedingungen geschaffen werden, die die MM Gruppe in die Lage versetzt, die gesetzlichen Anforderungen an Informationssicherheit und Datenschutz zeitnah, umfassend und inhaltlich konform zum Ansinnen des Gesetzgebers erfüllen zu können.

1.3. Informationssicherheitsstrategie

Die Strategie zur Umsetzung dieser Ziele umfasst folgende Punkte:

- Erweiterung des internen Kontrollsystems um informationssicherheitsrelevante Aspekte.
- Aufbau eines Informationssicherheitsmanagementsystems (ISMS) nach international anerkannten Standards.
- Aufbau eines Informationssicherheits-Risikomanagementsystems (IS-RM), das der Geschäftsführung die Informationen liefert, um risikoadäquate Entscheidungen im Zusammenhang mit Informationssicherheit treffen zu können.
- Etablierung eines Schulungs- und Awareness-Programms, um das technische IS Know-how und das IS-Bewusstsein den aktuellen Anforderungen anzupassen.
- Etablierung von geeigneten Key Performance Indikatoren (KPIs) und Auditmaßnahmen, um die operative Wirksamkeit und die Qualität des ISMS und der gesetzten operativen und technischen Maßnahmen kontinuierlich messen und verbessern zu können.
- Etablierung von Prozessen zur gesetzlich notwendigen Kommunikation mit Behörden und Kunden, bezüglich etwaiger Sicherheitsvorfälle oder zur Abfrage von personenbezogenen Daten und Informationen.

2. Geltungsbereich, Verankerung im Unternehmen

Die vorliegende Politik gilt in der Mayr-Melnhof Karton AG und allen Tochtergesellschaften, unabhängig vom Standort und bezieht sich auf sämtliche Tätigkeiten, Funktionen, Prozesse, Vermögens- und Informationswerte, die zur Erreichung der Unternehmensziele notwendig sind. Diese Politik ist allen Auftragnehmern zur Kenntnis zu bringen und findet bei der Beschaffung von neuen IT-Systemen Anwendung. Dies wird z.B. dadurch erreicht, dass die entsprechende Regelung in den Einkaufsbedingungen oder Planungsdokumenten zur Anwendung gebracht wird. Darüber hinaus kann der Regelungsinhalt dieser Politik im Einzelvertrag entsprechend berücksichtigt werden. Alle Mitarbeiter sind verpflichtet, die unten genannten Grundsätze und die daraus abgeleiteten Standards bei der Planung, der Entwicklung, der Beschaffung, der Errichtung, dem Betrieb und der Entsorgung von Informationswerten anzuwenden und einzuhalten.

3. Grundsätze

Das Informationssicherheitsmanagementsystem wird anhand der Norm ISO/IEC 27001:2013 und den BSI-Standards aufgebaut und kontinuierlich weiterentwickelt, wobei nachstehende Grundsätze zu berücksichtigen sind:

- Die Informationssicherheitsmaßnahmen und der Informationssicherheits-Risikomanagementprozess sind klar und eindeutig aus der Informationssicherheitspolitik ableitbar.
- Jeder Mitarbeiter soll die Informationen erhalten, die er benötigt, um seiner Tätigkeit nachkommen zu können. Ein Übermaß an Informationsbereitstellung wird durch technische oder organisatorische Maßnahmen vermieden. Um Fehler und Manipulationen Einzelner schon im Ansatz zu verhindern, sind miteinander unvereinbare Funktionen, Rollen und Verantwortungen zu trennen. Die Funktionstrennung soll Durchführungstätigkeiten von der Kontrolle dieser Tätigkeiten bezüglich ihrer operativen Wirksamkeit trennen. Ist eine Funktionstrennung nicht möglich, sind kompensierende Maßnahmen zu treffen. Diese Maßnahmen sind von den Leitungsorganen zu genehmigen.
- Der Informationszugriff wird protokolliert. Ein Zugriff auf Informationen ist im Rahmen der Aufgabenverteilung ausdrücklich geregelt.
- Die Einhaltung der Grundsätze sowie die operative Wirksamkeit des Informationssicherheitsmanagementsystems werden im Rahmen von internen und externen Audits sowie im Rahmen der regelmäßig durchgeführten Risikoanalyse überprüft. Die Ergebnisse werden dokumentiert. Auf Grundlage der Dokumentation werden konkrete Maßnahmen abgeleitet.
- Die Wahl der konkret zu implementierenden Informationssicherheitsmaßnahmen erfolgt in einem angemessenen Verhältnis zu den Risiken. Bei der Umsetzung der Maßnahmen wird dem Stand der Technik Rechnung getragen. Der Stand der Technik ist als ein sich kontinuierlich entwickelnder Innovationsprozess periodisch zu überprüfen und anzupassen.
- Für die Herstellung des risikoadäquaten Sicherheitsniveaus wird ein kombinierter Ansatz aus Basisschutzmaßnahmen und detaillierter Risikoanalyse verfolgt.
- Daten und Informationen werden bezüglich Vertraulichkeit, Integrität, Verfügbarkeit und Datenschutzrelevanz klassifiziert.
- Mitarbeitern wird regelmäßig das erforderliche Wissen zum bewussten Umgang mit Informationen durch Schulungen und Sensibilisierungsmaßnahmen vermittelt.
- Die Ausgestaltung der jeweiligen Grundsätze erfolgt in Unternehmensrichtlinien und Organisationsanweisungen.
- Für neu implementierte IT-Systeme sind die ISMS-Vorgaben unmittelbar anzuwenden. Für Bestandssysteme wird eine Überführung gesondert vereinbart.
- Für die kontinuierliche Weiterentwicklung des Informationssicherheitsmanagementsystems ist ein adäquates Kennzahlensystem zu pflegen.

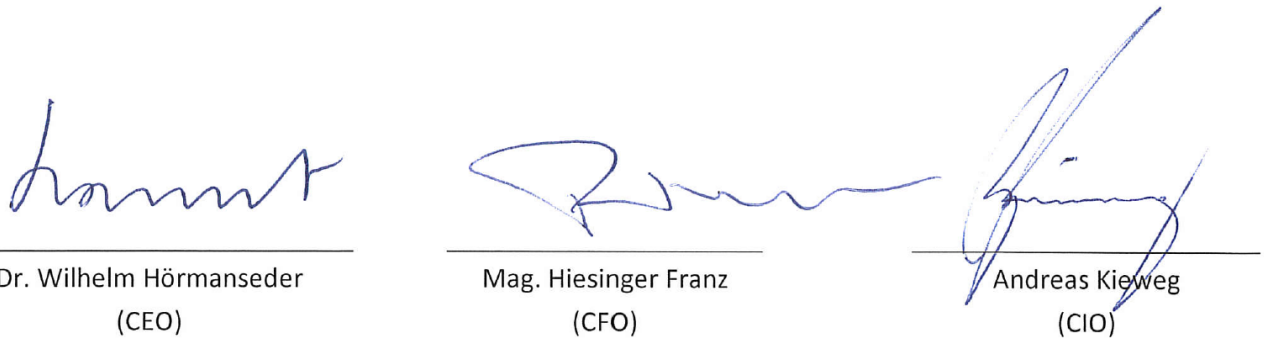
4. Durchsetzung und Sanktionierung

Die Leitungsorgane tragen die Verantwortung dafür, dass die Informationssicherheitsmaßnahmen entsprechend umgesetzt werden. Eine Einhaltung der Informationssicherheitsmaßnahmen wird aktiv kontrolliert. Wird im Rahmen der Kontrolle festgestellt, dass Mitarbeiter die Informationssicherheitsmaßnahmen nicht beachten, werden die zuständigen Leitungsorgane diese Mitarbeiter über deren Verpflichtung belehren. Gegebenenfalls wird die Missachtung sanktioniert.

5. Verbindlichkeitserklärung

Der Vorstand und die IT-Leitung der MM Gruppe definieren in der vorliegenden Informationssicherheitspolitik in der Version 1.10 vom 01.02.2018, Grundsätze die allen Entscheidungen und Maßnahmen in IT-Belangen im Unternehmen zugrunde zu legen sind. Diese Politik ist aus den übergeordneten Konzernstrategien abgeleitet und zu diesen harmonisiert. Sie ist wesentlicher Bestandteil zum Erreichen der Unternehmensziele und zur Umsetzung der festgelegten IT-Strategie. Die MM Gruppe verpflichtet sich die vorliegende Informationssicherheitspolitik zu verwirklichen, aufrechtzuerhalten und deren Wirksamkeit ständig zu verbessern.

Die vorliegende Informationssicherheitspolitik, sowie deren abgeleitete Richtlinien und Arbeitsanweisungen, werden mit Gültigkeit vom 01.03.2018 freigegeben, in Kraft gesetzt und für alle Beschäftigten der Mayr-Melnhof Karton AG und aller Tochterunternehmen, die sich im Mehrheitsbesitz der Mayr-Melnhof Karton AG befinden (einschließlich der externen, für das Unternehmen tätigen Mitarbeiter und für alle von der Corporate IT der MM Gruppe betreuten Unternehmen) für verbindlich erklärt.



Dr. Wilhelm Hörmanseder	Mag. Hiesinger Franz	Andreas Kieweg
(CEO)	(CFO)	(CIO)